Kaspersky Small Office Security 2

User Guide

PROGRAM VERSION: 9.1

Dear User!

Thank you for choosing our product. We hope that this document will help you in your work and will provide answers to most of the questions regarding this software product.

Warning! This document is the property of Kaspersky Lab: all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction and distribution of this document or parts hereof shall result in civil, administrative or criminal liability pursuant to the laws of the Russian Federation.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document and graphic images related to it may be used exclusively for informational, non-commercial, and personal purposes.

This document may be amended without additional notification. You can find the latest version of this document at the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document for which the rights are held by third parties, or for any potential damages associated with the use of such documents.

This document involves the registered trademarks and service marks which are the property of their respective owners.

Revision date: 10.12.2010

© 1997-2011 Kaspersky Lab ZAO. All Rights Reserved.

http://www.kaspersky.com
http://support.kaspersky.com/

CONTENTS

KASPERSKY LAB END USER LICENSE AGREEMENT 9

ABOUT THIS GUIDE 15

- In this document 15
- Document conventions 16

ADDITIONAL SOURCES OF INFORMATION 18

- Sources of information to research on your own 18
- Discussing Kaspersky Lab applications on the web forum 19
- Contacting the Sales Department 19
- Contacting the Documentation development group 19

KASPERSKY SMALL OFFICE SECURITY 2 20

- What's new 20
- Main application components and functions 21
- Distribution kit 23
- Hardware and software requirements 24

MANAGING THE LICENSE 26

- About End User License Agreement 26
- About license 26
- About activation code 27
- Viewing license information 28

APPLICATION INTERFACE 29

- Taskbar notification area icon 29
- Context menu 30
- Kaspersky Small Office Security main window 31
- Application settings window 33
- Notification windows and pop-up messages 34

STARTING AND STOPPING THE APPLICATION 36

- Enabling and disabling automatic launch 36
- Starting and stopping the application manually 36

OFFICE NETWORK PROTECTION STATUS 37

- Diagnostics and elimination of problems in your computer protection 37
- Enabling / disabling computer protection 38
- Pausing protection 39
- Using interactive protection mode 39

RESOLVING TYPICAL TASKS 41

- How to activate the application 41
- How to purchase or renew a license 42
- What to do when the application's notifications appear 43
- How to update application databases and modules 43
- How to scan critical areas of your computer for viruses 44
- How to scan a file, folder, disk, or another object for viruses 44
- How to perform full scan of your computer for viruses 46
- Scanning computer for vulnerabilities 46

How to check the protection status of an office computer network remotely 47
How to protect your personal data against theft 47
Protection against phishing 48
Virtual Keyboard 49
Password Manager 49
Data Encryption 51
What to do if you suspect an object of being infected with a virus 52
How to restore an object that has been deleted or disinfected by the application 52
What to do if you suspect your computer of being infected 53
How to create backup copies of your data 54
How to restrict access to Kaspersky Small Office Security settings 56
How to restrict computer and internet usage for different users 56
How to create and use Rescue Disk 57
Create Rescue Disk 57
Starting the computer from the Rescue Disk 59
What to do with a large number of spam messages 59
How to view the report on computer protection 60
How to restore application default settings 61
How to transfer application settings to another computer 61
ADVANCED APPLICATION SETTINGS 63
Scan 64
Virus scan 64
Vulnerability Scan 71
Update 72
Selecting an update source 73
Creating the update startup schedule 75
Rolling back the last update 76
Scanning Quarantine after update 76
Using the proxy server 76
Running updates under a different user account 77
File Anti-Virus 77
Enabling and disabling File Anti-Virus 78
Automatically pausing File Anti-Virus 78
Creating a protection scope 79
Changing and restoring security level 80
Changing the scan mode 81
Using heuristic analysis 81
Scan technology 81
Changing actions to be performed on detected objects 82
Scan of compound files 82
Scan optimization 83
Mail Anti-Virus 83
Enabling and disabling Mail Anti-Virus 85
Creating a protection scope 85
Changing and restoring security level 86
Using heuristic analysis 86
Changing actions to be performed on detected objects 87
Attachment filtering 87

Scan of compound files....87
Email scanning in Microsoft Office Outlook....88
Email scanning in The Bat!....88
Web Anti-Virus....89
Enabling and disabling Web Anti-Virus....90
Changing and restoring security level....91
Changing actions to be performed on detected objects....91
Blocking dangerous scripts....92
Checking URLs using the databases of suspicious and phishing addresses....92
Using heuristic analysis....92
Scan optimization....93
Kaspersky URL Advisor....93
Creating a list of trusted addresses....94
IM Anti-Virus....95
Enabling and disabling IM Anti-Virus....95
Creating a protection scope....95
Selecting the scan method....96
Anti-Spam....97
Enabling and disabling Anti-Spam....99
Changing and restoring security level....99
Training Anti-Spam....99
Scanning links in messages....102
Detecting spam by phrases and addresses. Creating lists....103
Regulating threshold values of spam rate....108
Using additional spam filtering features....108
Selecting the spam recognition algorithm....109
Adding a label to the message subject....109
Filtering email messages at the server. Mail Dispatcher....110
Excluding Microsoft Exchange Server messages from the scan....110
Configuring spam processing by mail clients....111
Anti-Banner....113
Enabling and disabling Anti-Banner....114
Selecting the scan method....114
Creating the lists of blocked and allowed banner addresses....114
Exporting and importing the lists of addresses....115
Security Zone....116
Enabling and disabling Security Zone....117
Placing applications into groups....117
Viewing activity of applications....119
Modifying a trust group....119
Security Zone rules....119
Protecting operating system resources and identity data....123
Proactive Defense....124
Enabling and disabling Proactive Defense....124
Creating a group of trusted applications....125
Using the dangerous activity list....125
Changing the dangerous activity monitoring rule....125
Rolling back a malicious program's actions....126
Network protection....126

Firewall....127
Network Attack Blocker....130
Encrypted connections scan....133
Network Monitor....135
Configuring the proxy server....135
Creating a list of monitored ports....135
Trusted zone....137
Creating a list of trusted applications....137
Creating the exclusion rules....138
Safe mode of applications execution....138
Running an application in safe mode....139
Creating the list of applications to run in safe mode....140
Creating a shortcut for program execution....141
Clearing Safe Run data....141
Using a shared folder....142
Quarantine and Backup....142
Storing quarantine and backup objects....143
Working with quarantined objects....143
Backup....145
Creating a backup storage area....146
Connecting an existing storage....146
Clearing a storage....147
Removing a storage....147
Creating a backup task....148
Running a backup task....148
Restoring data....149
Searching for backup copies....150
Viewing backup copy data....151
Viewing event report....151
Web Policy Management....152
Configure Web Policy Management for the user....153
Viewing reports of user's activity....161
Data Encryption....161
Creating and connecting an existing container....161
Locking and unlocking access to the data in the container....162
Adding files into container....163
Configuring container....164
Creating shortcut for quick access to the container....165
Management Console....165
Configuring remote management....166
Scanning the office network for viruses and vulnerabilities....167
Updating databases on networked computers remotely....167
Enabling / disabling protection components on networked computers....168
Remote Web Policy Management....169
Running backup tasks on networked computers....169
Managing licenses on networked computers remotely....170
Password Manager....170
Password Manager interface....172
Password Database management....176

Application settings configuration....189
Creating strong passwords....203
Using the portable version of Password Manager....204
Performance and compatibility with other applications....206
Selecting detectable threat categories....207
Advanced disinfection technology....207
Distributing computer resources when scanning for viruses....208
Application settings in full-screen mode. Presentation Mode....208
Battery saving....209
Kaspersky Small Office Security self-defense....209
Enabling and disabling self-protection....209
Protection against external control....210
Application appearance....210
Active interface elements....210
Kaspersky Small Office Security skin....211
News Agent....211
Additional Tools....212
Permanently Delete Data....212
Eliminating activity traces....213
Delete Unused Data....215
Browser Configuration....216
Reports....218
Creating a report for the selected component....218
Data filtering....219
Events search....219
Saving a report to file....220
Storing reports....220
Clearing application reports....221
Logging non-critical events....221
Configuring the reminder of report availability....221
Notifications....222
Enabling and disabling notifications....222
Configuring the notification method....223
Participating in the Kaspersky Security Network....224

VALIDATING KASPERSKY SMALL OFFICE SECURITY SETTINGS....225
Test "virus" EICAR and its modifications....225
Testing the HTTP traffic protection....226
Testing the SMTP traffic protection....227
Validating File Anti-Virus settings....227
Validating virus scan task settings....227
Validating Anti-Spam settings....228

CONTACTING THE TECHNICAL SUPPORT SERVICE....229
My Kaspersky Account....229
Technical support by phone....230
Creating a system state report....230
Creating a trace file....231
Sending data files....231
Executing AVZ script....232

APPENDIX 233
Subscription statuses 233
Working with the application from the command line 234
Activating the application 235
Starting the application 235
Stopping the application 236
Managing application components and tasks 236
Virus scan 238
Updating the application 240
Rolling back the last update 241
Exporting protection settings 241
Importing protection settings 242
Creating a trace file 242
Viewing Help 243
Return codes of the command line 243
GLOSSARY 244
KASPERSKY LAB 253
INFORMATION ABOUT THIRD-PARTY CODE 254
Program code 254
AGG (ANTI-GRAIN GEOMETRY) 2.4 255
BISON PARSER SKELETON 2.3 256
BOOST 1.30.0, 1.39.0, 1.43.0 256
BZIP2/LIBBZIP2 1.0.5 257
EXPAT 1.2, 2.0.1 257
FASTSCRIPT 1.9 257
GECKO SDK 1.8 257
INFO-ZIP 5.51 257
LIBJPEG 6B 258
LIBNKFM 2.0.5 259
LIBPNG 1.2.8, 1.2.29 259
LIBSPF2 1.2.9 259
LIBUNGIF 3.0 260
LIBXDR 260
NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE 260
NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER 261
NETWORK CONFIGURATION SAMPLE 261
OPENSSL 0.9.8D 261
PCRE 3.0, 7.4, 7.7 262
PROTOCOL BUFFER 263
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 263
TINICONV 1.0.0 263
WINDOWS TEMPLATE LIBRARY 7.5 269
WINDOWS TEMPLATE LIBRARY 8.0 272
ZLIB 1.2, 1.2.2 272
Other information 272
INDEX 273

KASPERSKY LAB END USER LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.** IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER CURRENT END USER LICENSE AGREEMENT.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

1.1. **Software** means software including any Updates and related materials.

1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.

1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.

1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, *"You"* further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term *"organization,"* without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.

1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.

1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.

2. Grant of License

2.1. You are given a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:

Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles.
If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of computers specified in licenses you have obtained *provided* that unless the licensing terms provide otherwise, each acquired license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.

2.2. If the Software was acquired on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package.
2.3. If the Software was acquired via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You acquired the License to the Software.
2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.
2.5. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was acquired on a physical medium) or specified during acquisition (if the Software was acquired via the Internet):
- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
- Technical Support via the Internet and Technical Support telephone hotline.

3. Activation and Term
3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.
3.2. If the Software was acquired on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement.
3.3. If the Software was acquired via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during acquisition.
3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement *provided that* the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline.
3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in User Manual.
3.6. If You have acquired the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.
3.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License without refunding the purchase price or any part thereof.
3.8. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.
3.9. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

4. Technical Support
4.1. The Technical Support described in Clause 2.5 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).

Technical support service: http://support.kaspersky.com
4.2. User's Data, specified in Personal Cabinet/My Kaspersky Account, can be used by Technical Support specialists only during processing User's request.

5. Information Collection
5.1. Having agreed with the terms and conditions of this Agreement You consent to provide information to the Rightholder about executable files and their checksums to improve Your security protection level.
5.2. In order to improve security awareness about new threats and their sources and in order to improve Your security protection level the Rightholder, with your consent, that has been explicitly confirmed in the Kaspersky Security Network Data Collection Statement, is expressly entitled to receives such information. You can deactivate the Kaspersky Security Network service during installation. Also, You can activate and deactivate the Kaspersky Security Network service at any time in the Software options page.
You further acknowledge and agree that any information gathered by Rightholder can be used to track and publish reports on security risk trends in the Rightholder's sole and exclusive discretion.
5.3. The Software does not process any personally identifiable data and does not combine the processing data with any personal information.
5.4. If you do not wish for the information collected by the Software to be sent to the Rightholder, You should not activate and/or de-activate the Kaspersky Security Network service.

6. Limitations
6.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.
6.2. You shall not transfer the rights to use the Software to any third party.
6.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder.
6.4. You shall not rent, lease or lend the Software to any third party.
6.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.
6.6. Your key file can be blocked in case You breach any of the terms and conditions of this Agreement.
6.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

7. Limited Warranty and Disclaimer
7.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual *provided however* that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.
7.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.
7.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

7.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.5 of this Agreement.
7.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 of this Agreement or after the License to use the Software is terminated for any reason.
7.6. THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER .

8. Exclusion and Limitation of Liability
8.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER AND/OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER AND/OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABILE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

9. GNU and Other Third Party Licenses
9.1. The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than

the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

10. Intellectual Property Ownership

10.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

10.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

11. Governing Law; Arbitration

11.1. This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 10 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

12. Period for Bringing Actions

12.1. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

13. Entire Agreement; Severability; No Waiver

13.1. This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to

insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

14. Rightholder Contact Information

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation
Tel: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Web site: www.kaspersky.com

© 1997-2011 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

ABOUT THIS GUIDE

This document is the Guide on configuring and operating Kaspersky Small Office Security 2 for Personal Computer and Kaspersky Small Office Security 2 for File Server.

The basic functions in Kaspersky Small Office Security 2 for Personal Computer and Kaspersky Small Office Security 2 for File Server are identical. The differences between Kaspersky Small Office Security 2 for Personal Computer and Kaspersky Small Office Security 2 for File Server are each described in the relevant section of the Guide.

Throughout the Guide, the terms "Kaspersky Small Office Security" and the "application" refer to both Kaspersky Small Office Security 2 for Personal Computer and Kaspersky Small Office Security 2 for File Server. Descriptions of functions and operations that differ in Kaspersky Small Office Security 2 for Personal Computer and Kaspersky Small Office Security 2 for File Server specify the full name of the application as appropriate.

This Guide is designed for product users.

Users of the application should be able to operate a personal computer at a basic level: to be familiar with the Microsoft Windows operating system interface and navigation within it, and to know how to use popular email and Internet programs, such as Microsoft Office Outlook and Microsoft Internet Explorer.

The aim of the document:

- to help users to configure the application with regard to user's required tasks;
- to provide a readily available source of information on application related issues;
- to provide alternative sources of information about the application and the means of getting technical support.

IN THIS SECTION:

In this document 15

Document conventions 16

IN THIS DOCUMENT

Kaspersky Small Office Security User Guide consists of the following main sections:

Additional sources of information

This section contains a description of the sources of additional information regarding the application, and Internet-resources where you can discuss the application, share ideas, ask questions and receive answers.

Kaspersky Small Office Security 2

This section describes the application's new features, and gives brief information about its individual components and basic functions. It describes the purpose of the distribution kit. This section contains hardware and software requirements which the computer must meet for the installation of Kaspersky Small Office Security.

Managing the license

This section contains information regarding the basic concepts used in the context of the application licensing. In this section, you will also learn about the automatic renewal of the license and where to view information regarding the current license.

Application interface

This section contains a description of the basic GUI components of the application: icon and context menu, main application window, settings windows, and notification windows.

Starting and stopping the application

This section contains information regarding the application's startup and shutdown.

Office network protection status

This section contains information about how to find out whether office network is currently protected, or if its security is under threat, as well as how to eliminate emerging threats. In this section, you can also find information about enabling, disabling, and pausing protection when working with Kaspersky Small Office Security.

Resolving typical tasks

This section contains instructions on the basic tasks encountered by most users when working with the application.

Advanced application settings

This section provides detailed information about each application component and describes the operation and configuration algorithms for each component.

Validating Kaspersky Small Office Security settings

This section contains recommendations in how to check if the application components run correctly.

Contacting the Technical Support service

This section contains recommendations with respect for making contact with Kaspersky Lab from My Kaspersky Account on the Technical Support Service website and by phone.

Appendix

This section includes reference information which complements the document text.

Glossary

This section contains the list of terms used in the document and their definitions.

DOCUMENT CONVENTIONS

Document conventions used in this guide are described in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted in red and enclosed in frames. Warnings contain important information, for example, related to computer operations critical to its safety.
It is recommended to use...	Notes are enclosed in frames. Notes contain additional and reference information.

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Example: ...	Examples are given by section, on a yellow background, and under the heading "Example".
Update means...	New terms are marked by italics.
ALT+F4	Names of keyboard keys appear in a bold typeface and are capitalized. Names of the keys followed by a "plus" sign indicate the use of a key combination.
Enable	Names of interface elements, for example, input fields, menu commands, buttons, etc., are marked in a bold typeface.
➧ *To configure a task schedule:*	Instructions' introductory phrases are in italics.
`help`	Texts in the command line or texts of messages displayed on the screen have a special font.
<IP address of your computer>	Variables are enclosed in angle brackets. The corresponding values are placed in each case instead of variables, angle brackets are omitted.

ADDITIONAL SOURCES OF INFORMATION

If you have any questions regarding selecting, purchasing, installing or using Kaspersky Small Office Security, various sources of information are available for your convenience. You can choose the most suitable information source, with regard to the question of importance and urgency.

IN THIS SECTION:

Sources of information to research on your own 18

Discussing Kaspersky Lab applications on the web forum 19

Contacting the Sales Department 19

Contacting the Documentation development group 19

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

Kaspersky Lab provides the following sources of information about the application:

- application page on the Kaspersky Lab website;
- application page on the Technical Support Service website (in the Knowledge Base);
- FastTrack Support service page;
- help system.

Application page on the Kaspersky Lab website

This page (http://www.kaspersky.com/small_office_security) provides you with general information on the application, its features and options.

Application page on the Technical Support Service website (Knowledge Base)

On this page (http://support.kaspersky.com/ksos) you will find the articles created by Technical Support Service specialists.

These articles contain useful information, advice and FAQs on purchasing, installing and using the application. They are sorted by subject, for example, Managing the product license, Configuring Update, or Eliminating operation failures. The articles may provide answers to the questions that concern not only this application but other Kaspersky Lab products as well. The articles may also contain news from the Technical Support Service.

FastTrack Support service

On this service page, you can find the database of FAQs with answers regarding the application's operation. To use this service, you need an Internet connection.

To go to the service page, in the main application window, click the **Support** link and in the window that opens click the **FastTrack Support** button.

Help system

The application installation package includes the file of full and context help that contains information about how to manage computer protection (view protection status, scan various computer areas for viruses, and execute other

tasks). Besides, in the file of full and context help, you can find information on each application window such as the list of its proper settings and their description, and the list of tasks to execute.

To open the help file, click the **Help** button in the required window, or press the **F1** key.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other users in our forum at http://forum.kaspersky.com.

In this forum you can view existing topics, leave your comments, create new topics and use the search engine.

CONTACTING THE SALES DEPARTMENT

If you have questions about selecting or purchasing Kaspersky Small Office Security or extending your license, you can contact the Sales Department (http://www.kaspersky.com/contacts).

You can also send your questions to the Sales Department by email at sales@kaspersky.com.

CONTACTING THE DOCUMENTATION DEVELOPMENT GROUP

If you have any questions regarding documentation, have found an error or you would like to leave feedback, you can contact the Documentation development group. To contact Documentation development group, send a message to docfeedback@kaspersky.com. Please use "Kaspersky Help Feedback: Kaspersky Small Office Security" as the subject line in your message.

KASPERSKY SMALL OFFICE SECURITY 2

Kaspersky Small Office Security 2 is a solution for small organizations with their own local network of no more than ten computers. Kaspersky Small Office Security 2 protects the computer network from viruses and other threats.

Kaspersky Small Office Security 2 consists of two parts:

- Kaspersky Small Office Security 2 for Personal Computer is installed on personal computers under the Microsoft Windows operating system. The application provides maximum protection for data on the computer, safe browsing on the Internet, flexible configuration of policies for different users on the computer and the Internet, and tools for the remote management of office network computers.

- Kaspersky Small Office Security 2 for File Server is installed on file servers under the Microsoft Windows operating system. The application provides protection for data on the computer and tools for the remote management of office network computers.

Kaspersky Small Office Security 2 for Personal Computer and Kaspersky Small Office Security 2 for File Server are included in the common installation package. When installing the application, the Setup Wizard defines which application should be installed on your computer - Kaspersky Small Office Security 2 for Personal Computer or Kaspersky Small Office Security 2 for File Server - based on the information about the operating system.

The basic features of the components and functions of Kaspersky Small Office Security 2 for Personal Computer and Kaspersky Small Office Security 2 for File Server are identical. Some components and functions in Kaspersky Small Office Security 2 for Personal Computer are not available in Kaspersky Small Office Security 2 for File Server.

IN THIS SECTION:

What's new 20

Main application components and functions 21

Distribution kit 23

Hardware and software requirements 24

WHAT'S NEW

The following innovations have been introduced in Kaspersky Small Office Security 2:

- Updated anti-virus kernel for more effective detection of viruses.

- Improved user interface for easier control.

- New Data Encryption component for the encryption and storage of data in encrypted form; this protects important information from third parties.

- New Password Manager component (only in Kaspersky Small Office Security 2 for Personal Computer) for the storage in encrypted form of various personal data (for example, user names, passwords, addresses, telephone and credit card numbers).

- New Backup component for the creation of backup copies of data.

- New Management Console component for the remote management of computer security in the office network.

- New Virtual Keyboard to prevent the interception of entered data (for example, passwords).
- Users can now participate in the Kaspersky Security Network and gain access to Kaspersky Lab's online knowledge database, which contains information about the security of files, online resources, and software.

MAIN APPLICATION COMPONENTS AND FUNCTIONS

Kaspersky Small Office Security provides all-inclusive protection for your office network. All-inclusive protection means computer protection, data protection and user protection, as well as remote management of Kaspersky Small Office Security on all network computers.

Kaspersky Small Office Security incorporates various functional modules to perform all-inclusive protection tasks.

Computer Protection

Protection components are designed to protect the computer against known and new threats, network and hacker attacks, and spam and other unsolicited information. Every type of threat is handled by an individual protection component (see the description of components in this section). Components can be enabled or disabled independently of one another and configured accordingly.

In addition to the constant protection provided by the security components, we recommend that you regularly *scan* your computer for viruses. This is necessary in order to rule out the possibility of spreading malicious programs that have not been discovered by protection components, for example, because of a low security level set, or for other reasons.

To keep Kaspersky Small Office Security up to date, you need to *update* the databases and software modules used by the application.

When the safety of any application raises doubts, they can be run in a *safe environment* (only in Kaspersky Small Office Security 2 for Personal Computer).

Certain specific tasks that need to be performed occasionally can be performed with the help of *additional tools and wizards*, such as configuring Microsoft Internet Explorer or erasing the traces of user activity in the system.

The following protection components provide defense for your computer in real time:

File Anti-Virus

File Anti-Virus prevents infection of the computer's file system. The component starts upon startup of the operating system, continuously remains in the computer's RAM, and scans all files being opened, saved, or launched on your computer and all connected drives. Kaspersky Small Office Security intercepts each attempt to access a file and scans the file for known viruses. The file can only be processed further if the file is not infected or is successfully treated by the application. If a file cannot be disinfected for any reason, it will be deleted. A copy of the file will be saved in Backup, or moved to Quarantine.

Mail Anti-Virus (only in Kaspersky Small Office Security 2 for Personal Computer)

Mail Anti-Virus scans incoming and outgoing email messages on your computer. The email is available to the addressee only if it does not contain dangerous objects.

Web Anti-Virus (only in Kaspersky Small Office Security 2 for Personal Computer)

Web Anti-Virus intercepts and blocks scripts on websites if they pose a threat. All web traffic is also subject to monitoring. Additionally, the component blocks access to malicious websites.

IM Anti-Virus (only in Kaspersky Small Office Security 2 for Personal Computer)

IM Anti-Virus ensures the safe use of instant messengers. The component protects information that comes to your computer via IM protocols. IM Anti-Virus ensures safe operation of various applications for instant messaging.

Proactive Defense (only in Kaspersky Small Office Security 2 for Personal Computer)

Proactive Defense allows to detect a new malicious program before it performs its malicious activity. The component's operation is based on monitoring and analyzing the behavior of all applications installed on your computer. Depending on the actions being performed, Kaspersky Small Office Security makes a decision whether the application is potentially dangerous or not. So your computer is protected not only from known viruses, but also from new ones that have not yet been discovered.

Security Zone (only in Kaspersky Small Office Security 2 for Personal Computer)

Security Zone logs the actions performed by applications in the system, and manages the applications' activities, based on which group the component assigns them to. A set of rules is defined for each group of applications. These rules manage the applications' access to various operating system resources.

Firewall

The Firewall ensures security for your work in local networks and on the Internet. The component filters all network activities using two types of rule: *rules for applications* and *packet rules*.

Network Monitor

The component is designed for viewing information about network activity in real-time.

Network Attack Blocker

The Network Attack Blocker loads during the operating system launch, and scans incoming network traffic for activities characteristic of network attacks. As soon as an attempt to attack the computer is detected, Kaspersky Small Office Security blocks any network activity of the attacking computer towards your computer.

Anti-Spam (only in Kaspersky Small Office Security 2 for Personal Computer)

Anti-Spam integrates into the mail client installed on your computer, and monitors all incoming email messages for spam. All messages containing spam are marked with a special header. The option of configuring Anti-Spam for spam processing (deleting automatically, moving to a special folder, etc.) is also provided.

Anti-Phishing (only in Kaspersky Small Office Security 2 for Personal Computer)

A component integrated in Web Anti-Virus, Anti-Spam and IM Anti-Virus, which checks web addresses to see if they are included in the list of phishing and suspicious web addresses.

Anti-Banner (only in Kaspersky Small Office Security 2 for Personal Computer)

Anti-Banner blocks advertising information located on banners built into interfaces of various programs installed on your computer, or displayed online.

Data protection

The Backup, Data Encryption and Password Manager functions are designed to protect data against loss, unauthorized access and theft.

Backup

Data stored on a computer can be lost due to various issues, such as impact of a virus, information modification or deletion by another user, etc. To avoid losing important information, you should regularly back up data.

The Backup function creates backup copies of objects in a special storage on the selected device. To do so, you should configure backup tasks. After running the task manually or automatically, according to a schedule, backup copies of selected files are created in the storage. If necessary, the required version of the saved file can be restored from the backup copy. Thus, regular backup ensures additional security of data.

Data Encryption

Confidential information, which is saved in electronic mode, requires additional protection from unauthorized access. Storing data in an encrypted container provides this protection.

Data Encryption allows creating special encrypted containers on the chosen drive. In the system, such containers are displayed as virtual removable drives. To access the data in the encrypted container, a password should be entered.

Password Manager (only in Kaspersky Small Office Security 2 for Personal Computer)

At the moment, registration and entering account data for authentication are required to access the majority of services and resources. For security reasons, it is not recommended to use identical user accounts for different resources, or write down your user name and password. As a result, today's user is not able to remember huge amounts of account data, which makes safe storing of passwords particularly up-to-date.

Password Manager makes it possible to store different personal data in encrypted form (for example, user names, passwords, addresses, phone and credit card numbers). Data access is protected with a single Master Password. After entering the Master Password, Password Manager can automatically fill in the fields of different authorization forms. Thus, you should remember only one Master Password to manage all account data.

Web Policy Management (only in Kaspersky Small Office Security 2 for Personal Computer)

Web Policy Management ensures compliance with the company's rules and regulations regarding use of the computer and the Internet.

Web Policy Management allows the configuration of flexible access restrictions to online resources and application for different computer users. It also lets you view statistical reports on controlled user activity.

Management Console

Office network often comprises several computers, which makes it difficult to manage network security. The vulnerability of one computer puts in jeopardy the whole network.

Management Console allows starting virus scan tasks and update tasks for the whole network or for selected computers, manage the backup copying of data, and configure Web Policy Management settings on all computers within the network immediately from your workspace. This ensures remote security management of all computers within office network.

DISTRIBUTION KIT

You can purchase the boxed version of Kaspersky Small Office Security from our resellers, or purchase it online from Internet shops, such as the **eStore** section of http://www.kaspersky.com.

If you buy the boxed version of the program, the package will include:

- A sealed envelope with the installation disk, containing the software and documentation. The documentation includes PDF versions of the User Guide and the Installation Guide.
- Installation Guide in printed form.
- License Agreement (depending on the region).
- Activation card containing an activation code and the application activation manual.

The End-User License Agreement is a legal agreement between you and Kaspersky Lab that specifies the terms under which you may use the software you have purchased.

Read through the EULA carefully!

If you do not agree with the terms of the EULA, you can return your boxed product to the partner from whom you purchased it and be reimbursed the amount you paid for the program, provided that the envelope containing the installation disk is still sealed.

By opening the sealed installation disk, you accept all the terms of the EULA.

Before breaking the seal on the installation disk envelope, carefully read through the EULA.

If you buy Kaspersky Small Office Security from eStore, you will download the product from the Kaspersky Lab website; the User Guide and Installation Guide are included with the installation package. You will be sent an activation code by email after your payment has been received.

HARDWARE AND SOFTWARE REQUIREMENTS

To run Kaspersky Small Office Security, the computer should meet the following minimum requirements specified in this section:

Common requirements for Kaspersky Small Office Security 2 for File Server and Kaspersky Small Office Security 2 for Personal Computer:

- 500 MB free hard drive space.
- CD-ROM (to install Kaspersky Small Office Security from the distribution CD).
- Microsoft Internet Explorer 6.0 or higher (for updating application's databases and software modules via Internet).
- Microsoft Windows Installer 2.0.
- Mouse pointing device.
- Internet connection to activate Kaspersky Small Office Security.

The file server on which Kaspersky Small Office Security 2 for File Server is installed should meet the following requirements:

- Microsoft Windows Server 2008 R2 Foundation, Microsoft Windows Server 2008 R2 Standard:
  - Intel Pentium 1.4 GHz 64-bit (x64) or a dual core 1.3 GHz processor or higher (or a compatible equivalent).
  - 512 MB RAM.
- Microsoft Windows Small Business Server 2011 Essentials ("Aurora"):
  - Intel Pentium 2 GHz 64-bit (x64) processor or higher (or a compatible equivalent).
  - 4 GB RAM.
- Microsoft Windows Small Business Server 2011 Standard ("SBS 7"):
  - Intel Pentium 2 GHz 64-bit (x64) processor or higher (or a compatible equivalent).
  - 4 GB RAM.

At the time of release, Kaspersky Small Office Security 2 does not support Microsoft Windows Small Business Server 2011 Essentials ("Aurora") and Microsoft Windows Small Business Server 2011 Standard ("SBS 7") operating systems, because they are not yet officially released by Microsoft. For up-to-date information about the support of these operating systems, refer to the Kaspersky Lab website, the page providing information about Kaspersky Small Office Security (http://www.kaspersky.com/small-office-security).

The personal computer on which Kaspersky Small Office Security 2 for Personal Computer is installed should meet the following requirements:

- Microsoft Windows XP Home Edition Service Pack 3, Microsoft Windows XP Professional Service Pack 3, Microsoft Windows XP Professional x64 Edition Service Pack 2:
  - Intel Pentium 300 MHz processor or higher (or a compatible equivalent).
  - 256 MB RAM.
- Microsoft Windows Vista Home Basic (32-bit / 64-bit, Service Pack 2), Microsoft Windows Vista Home Premium (32-bit / 64-bit, Service Pack 2), Microsoft Windows Vista Business (32-bit / 64-bit, Service Pack 2), Microsoft Windows Vista Enterprise (32-bit / 64-bit, Service Pack 2), Microsoft Windows Vista Ultimate (32-bit / 64-bit, Service Pack 2):
  - Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent).
  - 1 GB RAM.
- Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:
  - Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent).
  - 1 GB RAM (for 32-bit systems); 2 GB RAM (for 64-bit systems).

Restrictions for 64-bit operating systems:

- You cannot enable Safe Run when working under a Microsoft Windows XP (64-bit) operating system. Safe Run is restricted when working in Microsoft Windows Vista (64-bit) and Microsoft Windows 7 (64-bit) operating systems.
- Password Manager cannot run under 64-bit operating systems.

MANAGING THE LICENSE

This section contains information regarding the basic concepts used in the context of the application licensing. In this section, you will also learn about the automatic renewal of the license and where to view information regarding the current license.

IN THIS SECTION:

About End User License Agreement 26

About license 26

About activation code 27

Viewing license information 28

ABOUT END USER LICENSE AGREEMENT

The *End User License Agreement* – is an agreement between natural or legal person lawfully in possession of a copy of an application. The EULA is included in each Kaspersky Lab application. It contains a detailed description of rights and Kaspersky Small Office Security usage restrictions.

According to the EULA, when you purchase and install a Kaspersky Lab application, you get an unlimited right to own its copy.

ABOUT LICENSE

License is a right to use Kaspersky Small Office Security and the related additional services offered by Kaspersky Lab or its partners.

Each license is defined by its expiry date and a type.

License term – a period during which the additional services are offered:

- technical support;
- updating databases and application modules.

The services provided depend on the license type.

The following license types are provided:

- *Trial* – a free license with a limited validity period, for example, 30 days, offered to become familiar with Kaspersky Small Office Security.

  A trial license can only be used once and cannot be used after a commercial license!

  A trial license is supplied with the trial version of the application. If you have a trial license, you can only contact Technical Support Service if your question is about activating the product or purchasing a commercial license. As soon as the trial license expires, all Kaspersky Small Office Security features become disabled. To continue using the application, you should activate it (see section "How to activate the application" on page 41).

- *Commercial* – a commercial license with a limited validity period (for example, one year), offered upon purchase of Kaspersky Small Office Security. Each license is assigned a number of hosts on which you can install Kaspersky Small Office Security with this license.

  If a commercial license is activated, all application features and additional services are available.

  As soon as a commercial license expires, Kaspersky Small Office Security remains a full-featured application, but the anti-virus databases are not updated. You can still scan your computer for viruses and use the protection components, but only using the databases that you had when the license expired. Two weeks before the license expiration date, the application will notify you of this event so you can renew the license in advance (see section "How to purchase or renew a license" on page 42).

- *Commercial with an update subscription* and *commercial with an update and protection subscription* – a paid license with flexible management: you can suspend and resume the subscription, extend its validity period in the automatic mode and cancel the subscription. A license with subscription is distributed by service providers. You can manage the subscription from the user's Personal Cabinet on the service provider's website.

  The validity period of a subscription can be limited (for example, to one year) or unlimited. If a subscription with a limited validity period is activated, you should renew it on your own when it expires. A subscription with an unlimited validity period is extended automatically subject to timely prepayment to the provider.

  If the subscription term is limited, when it expires, you will be offered a grace period for subscription renewal, during which the full functionality of the program will be maintained.

  If the subscription is not renewed, when grace period expires, Kaspersky Small Office Security ceases to update the application databases (for licenses with an update subscription) and stops performing computer protection or executing scan tasks (for licenses with a protection subscription).

  When using the subscription, you will not be able to use another activation code to renew the license. This is only possible after the subscription expiry date.

  If already have an activated license with a limited term at the time of subscription activation, it is substituted with the subscription license. To cancel the subscription, contact the service provider from whom you purchased Kaspersky Small Office Security.

  Depending on the subscription provider, the set of available actions to be performed on the subscription may vary. Also, the grace period when subscription renewal is available, is not provided by default.

ABOUT ACTIVATION CODE

Activation code is the code supplied with a Kaspersky Small Office Security commercial version. This code is required for activation of the application.

The activation code represents a sequence of Latin characters and digits separated by hyphens into four groups of five symbols. For example, 11111-11111-11111-11111.

You can activate Kaspersky Small Office Security 2 for Personal Computer or Kaspersky Small Office Security 2 for File Server using the activation code:

- If the activation code was issued for Kaspersky Small Office Security 2 for Personal Computer, you can use it to activate Kaspersky Small Office Security 2 for Personal Computer. Kaspersky Small Office Security 2 for File Server cannot be activated with this activation code.

- If the activation code was issued for Kaspersky Small Office Security 2 for File Server, you can use it to activate Kaspersky Small Office Security 2 for File Server. Kaspersky Small Office Security 2 for Personal Computer cannot be activated with this activation code.

- If the activation code was issued for Kaspersky Small Office Security 2 for File Server and Kaspersky Small Office Security 2 for Personal Computer, you can use it to activate both Kaspersky Small Office Security 2 for File Server and Kaspersky Small Office Security 2 for Personal Computer.

You can also activate the application using an activation code for a previous version of the application:

- If the activation code was issued for Kaspersky Anti-Virus 6.0 for Windows Workstations, it can be used to activate Kaspersky Small Office Security 2 for Personal Computer. Kaspersky Small Office Security 2 for File Server cannot be activated with this activation code.

- If the activation code was issued for Kaspersky Anti-Virus 6.0 for Windows Servers and Kaspersky Anti-Virus 6.0 for Windows Workstations, it can be used to activate both Kaspersky Small Office Security 2 for File Server and Kaspersky Small Office Security 2 for Personal Computer.

The number of personal computers on which Kaspersky Small Office Security 2 for Personal Computer can be installed depends on the license purchased; the number is usually five or ten personal computers.

The number of file servers on which Kaspersky Small Office Security 2 for File Server can be installed also depends on the license purchased, and is usually one file server.

If you purchase the boxed version of the application, the number of personal computers and files servers on which it can be installed is indicated on the box. If you purchase the application online , the number is displayed on the web page with information about the purchase.

After the application is installed, the number of personal computers and file servers on which it can be installed is displayed in the License management window (see Section "View license information" on page 28).

VIEWING LICENSE INFORMATION

To view information about the active license:

1. Open the main application window.

2. Click the **License** button in the bottom part of the window to open the **License management** window.

   In this window, you can view information about the active license, start the application activation (see section "How to activate the application" on page 41), purchase a new license, or renew your current one (see section "How to purchase or renew a license" on page 42).

APPLICATION INTERFACE

This section will discuss the basic features of Kaspersky Small Office Security interface.

IN THIS SECTION:

Taskbar notification area icon 29

Context menu 30

Kaspersky Small Office Security main window 31

Application settings window 33

Notification windows and pop-up messages 33

TASKBAR NOTIFICATION AREA ICON

Immediately after installing Kaspersky Small Office Security, its icon will appear in the Microsoft Windows taskbar notification area.

The icon has the following basic purposes:

- It is an indicator of the application's operation.
- It provides access to the context menu, main application window and the news window.

Indication of the application activity

This icon serves as an indicator of the application's operation. It also indicates the protection status and shows a number of basic functions currently being performed by the application:

– scanning an email message;

– scanning web traffic;

– updating databases and application modules;

– computer needs to be restarted to apply updates;

– a failure occurred in the operation of an application component.

The icon is animated by default: for example, during the email message scan, a tiny letter symbol blinks against the application icon; when the update is in progress, you can see a revolving globe. Animation can be deactivated (see page 210).

When the animation is disabled, the icon can take the following form:

(colored symbol) – all or certain protection components are activated;

(black-and-white symbol) – all protection components are disabled.

Access to the context menu and application windows

You can use the icon to open the context menu (see page 30) and the main application window (see page 31).

- *To open the context menu,*

  hover the cursor over the icon and right-click the area.

- *To open the main application window,*

  hover the cursor over the icon and left-click the area.

If news from Kaspersky Lab is available, the icon appears in the Microsoft Windows taskbar notification area. Double-click this icon to open the News window (see page 211).

CONTEXT MENU

You can run basic protection tasks from the context menu.

The Kaspersky Small Office Security menu contains the following items:

- **Update** – runs the update of application databases and modules.
- **Full Scan** – starts a full scan of your computer for malware (see page 46).
- **Virus Scan** – starts a scan of selected objects for malware (see page 44).
- **Virtual Keyboard** – displays the Virtual Keyboard (see page 49).
- **Kaspersky Small Office Security** – opens the main application window (see page 31).
- **Settings** – opens the application settings window. (see page 33).
- **Activation** – starts the Kaspersky Small Office Security activation wizard. This menu item is only available if the application has not been activated.
- **About** – opens a window containing information about the application.
- **Pause / Resume protection** – temporarily turns off / on the real-time protection components. This menu option does not affect the application's updates, or the execution of virus scans.
- **Enable / Pause Web Policy Management** – temporarily disables / enables control of all users. This menu item is only available if the Web Policy Management component is installed (only in Kaspersky Small Office Security 2 for Personal Computer).
- **Block network traffic / Unblock network traffic** – temporarily blocks / unblocks all network connections on your computer.

- **Exit** – closes Kaspersky Small Office Security. When this option is selected, the application will be discarded from the computer's RAM.

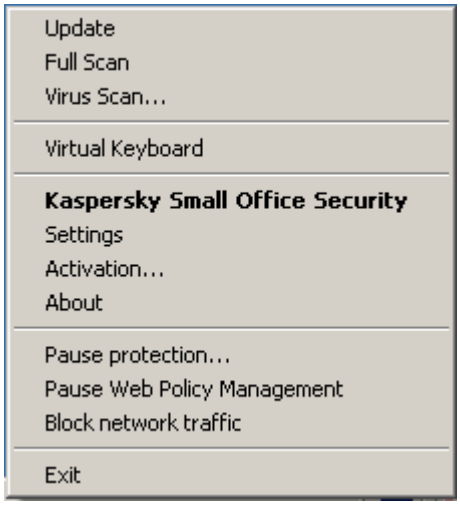

Figure 1. Context menu

If a virus scan or update task is running at the moment that you open the context menu, its name as well as its progress status (percentage complete) is displayed in the context menu. When you select a menu item with the name of a task, you can switch to the main window with a report of current task run results.

To open the context menu,

hover over the application icon in the taskbar notification area with the cursor and right-click it with the mouse.

KASPERSKY SMALL OFFICE SECURITY MAIN WINDOW

The main window contains interface elements that provide access to all the main features of the application.

The main window can be divided into three parts.

- The top part of the window indicates your computer's current protection status.

Figure 2. Current computer protection status

There are three possible values of protection status: each of them is indicated with a certain color. Green indicates that your computer's protection is at the correct level, while yellow and red indicate that there are various security threats. In addition to malicious programs, threats include obsolete application databases, disabled protection components, minimum protection settings, etc.

Security threats must be eliminated as they appear (see section "Diagnostics and elimination of problems in your computer protection" on page 37).

- The left part of the window provides quick access to any function of the application, including virus scan tasks, updates, etc.

- The right part of the window contains information about the application function selected in the left part, allows to configure its settings, provides tools for executing virus scan tasks, retrieving updates etc.

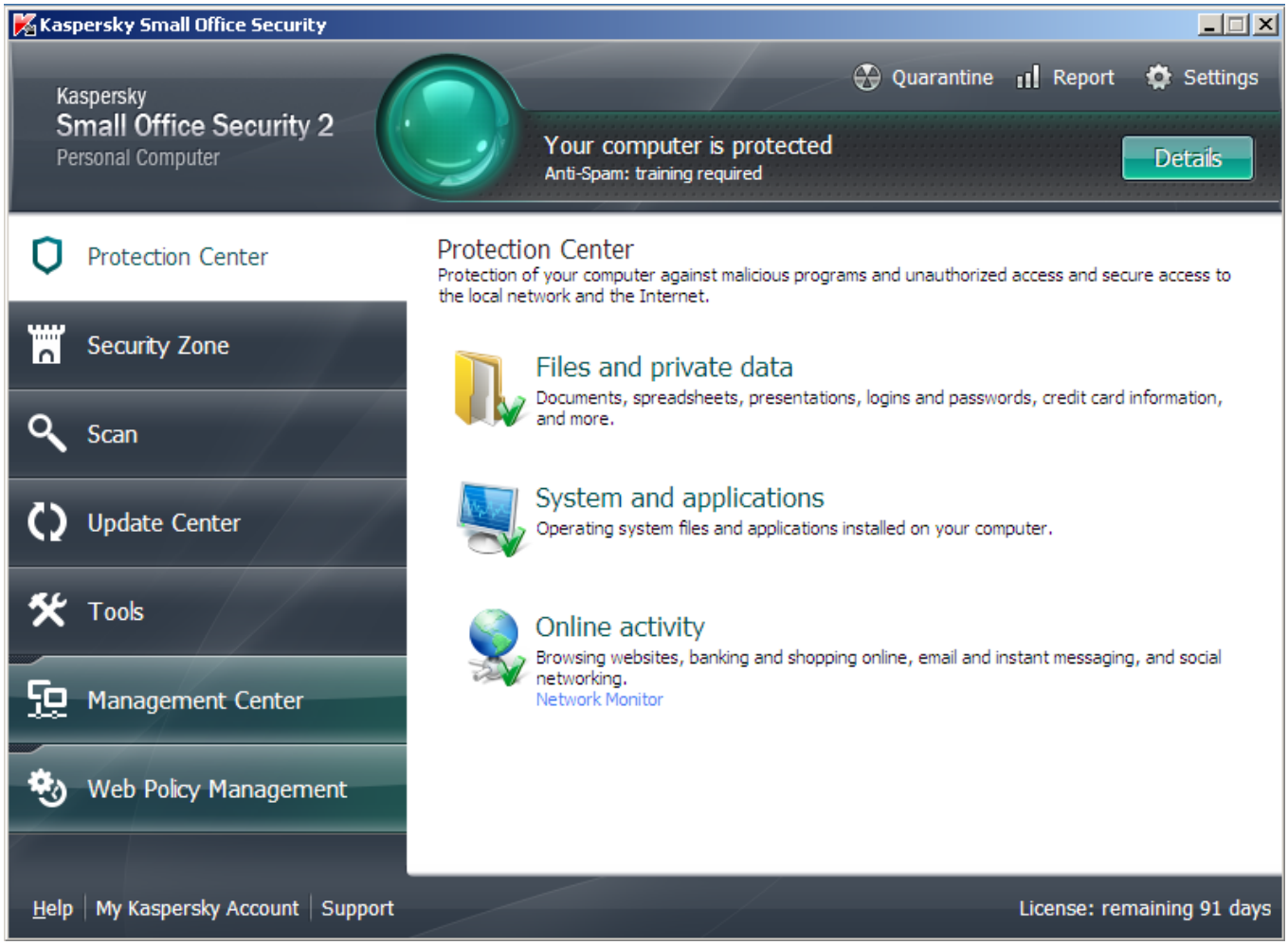

Figure 3. Main application window

You can also use the following buttons and links:

- **Quarantine** – start working with quarantined objects.
- **Report** – open the list of events occurred during application operation.
- **Settings** – to open the computer protection settings window.
- **Help** – to view the Kaspersky Small Office Security help system.
- **My Kaspersky Account** – to enter the user's personal cabinet (https://my.kaspersky.com) at the Technical Support Service's website.
- **Support** – to open the window containing information about the system and links to Kaspersky Lab information resources (Technical Support Service website, forum).
- **License** – Kaspersky Small Office Security activation, and license renewal.

You can change the appearance of (see section "Application's appearance" on page 210) Kaspersky Small Office Security by creating and using various graphics and color schemes.

APPLICATION SETTINGS WINDOW

The Kaspersky Small Office Security settings window is designed for configuring the entire application, separate protection components, scan and update tasks, and for running other advanced configuration tasks (see page 63). The application settings window consists of three parts:

- the top part contains the categories of tasks and functions of Kaspersky Small Office Security;
- the left part of the window provides access to the general tasks and functions of Kaspersky Small Office Security in the selected category;
- the right part of the window contains a list of settings for the function or task selected in the left part of the window.

The settings configuration window may be opened from the main window (see page 31) or using the context menu (see page 30). To open the configuration window, click the **Settings** link in the top part of the main window, or select the appropriate option in the application's context menu.

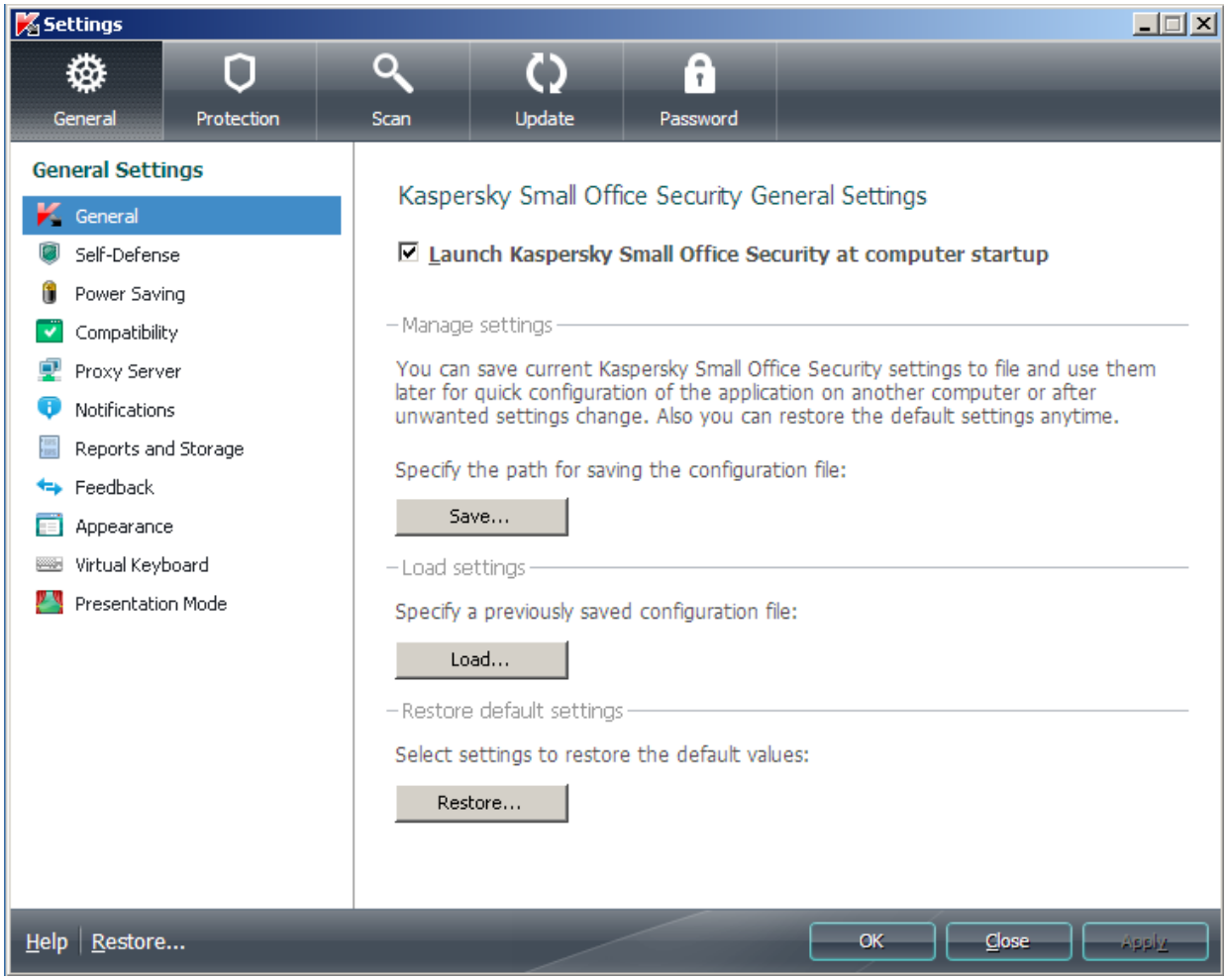

Figure 4. Configuring Kaspersky Small Office Security settings

NOTIFICATION WINDOWS AND POP-UP MESSAGES

Kaspersky Small Office Security notifies you of important events occurring during its operation, using *notification windows* and *pop-up messages* that appear over the application icon in the taskbar notification area.

Notification windows are displayed by Kaspersky Small Office Security when various actions can be taken in connection with an event: for example, if a malicious object is detected, you can block access to it, delete, or try to disinfect it. The application offers you to select one of the available actions. A notification window only disappears from the screen if you select one of the actions.

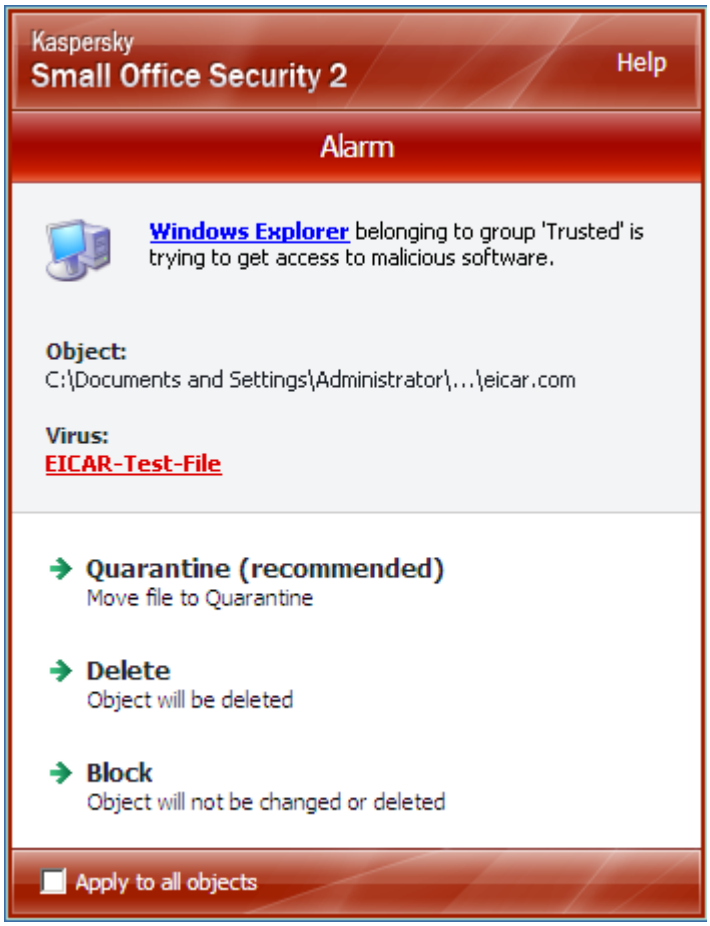

Figure 5. The Notifications window

Pop-up messages are displayed by Kaspersky Small Office Security in order to inform you of events that do not require selection of an action. Some pop-up messages contain links that you can use to take an action offered by the application: for example, run the update of the databases, or initiate the activation of the application). Pop-up messages automatically disappear from the screen soon after they appear.

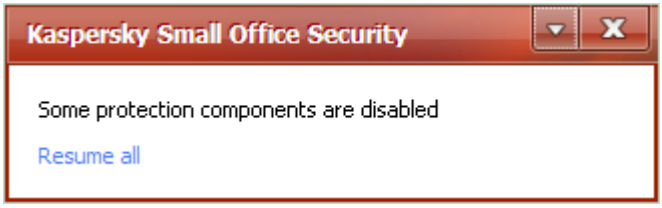

Figure 6. Pop-up message

Depending on how critical the event is for computer security, you might receive the following types of notification:

- Critical notifications – inform you of events of critical importance from the viewpoint of computer security: for example, detection of a malicious object or dangerous activity in the system. Notification windows and pop-up messages of this type are red-colored.

- Important notifications – inform you of events which are potentially important from the viewpoint of computer security: for example, detection of a potentially infected object or suspicious activity in the system. Notification windows and pop-up messages of this type are yellow-colored.

- Informational messages – inform you of events that are non-critical from the viewpoint of security. Notification windows and pop-up messages of this type are green-colored.

STARTING AND STOPPING THE APPLICATION

After Kaspersky Small Office Security has been installed, it starts automatically. The application is launched automatically each time the operating system starts.

IN THIS SECTION:

Enabling and disabling automatic launch 36

Starting and stopping the application manually 36

ENABLING AND DISABLING AUTOMATIC LAUNCH

Automatic launch of the application means that Kaspersky Small Office Security launches after the operating system startup. This is the default start mode.

- *To disable automatic launch of the application:*

  1. Open the main application window.
  2. In the top part of the window, click the **Settings** link.
  3. In the left part of the window, in the **General Settings** section, select the **General** subsection.
  4. In the right part of the window, uncheck the **Launch Kaspersky Small Office Security at computer startup** box.

STARTING AND STOPPING THE APPLICATION MANUALLY

Kaspersky Lab specialists do not recommend that you stop Kaspersky Small Office Security, because protection of your computer and personal data will be at risk. If disabling protection is really necessary, you are advised to pause your computer protection (see page 39) for the required period without closing the application.

Kaspersky Small Office Security should be started manually if you have disabled automatic launch of the application (see page 36).

- *To launch the application manually,*

  in the **Start** menu, select **Programs** → **Kaspersky Small Office Security** → **Kaspersky Small Office Security**.

- *To exit the application,*

  right-click to open the context menu of the application icon in the taskbar notification area and select **Exit**.

OFFICE NETWORK PROTECTION STATUS

This section contains information about how to find out whether office network is currently protected, or if its security is under threat, as well as how to eliminate emerging threats.

In this section, you can also find information about enabling, disabling, and pausing protection when working with Kaspersky Small Office Security.

DIAGNOSTICS AND ELIMINATION OF PROBLEMS IN YOUR COMPUTER PROTECTION

Problems with computer protection are indicated by the protection status indicator located in the top part of the Kaspersky Small Office Security main window. The indicator changes color depending upon the host protection status: green means that the computer is protected, yellow indicates protection-related problems, red alerts of serious threats to computer security. You are advised to fix the problems and security threats immediately.

Clicking the protection status indicator in the main application window opens the **Protection state** window (see the figure below) containing detailed information about the status of computer protection and troubleshooting suggestions for the detected problems and threats.

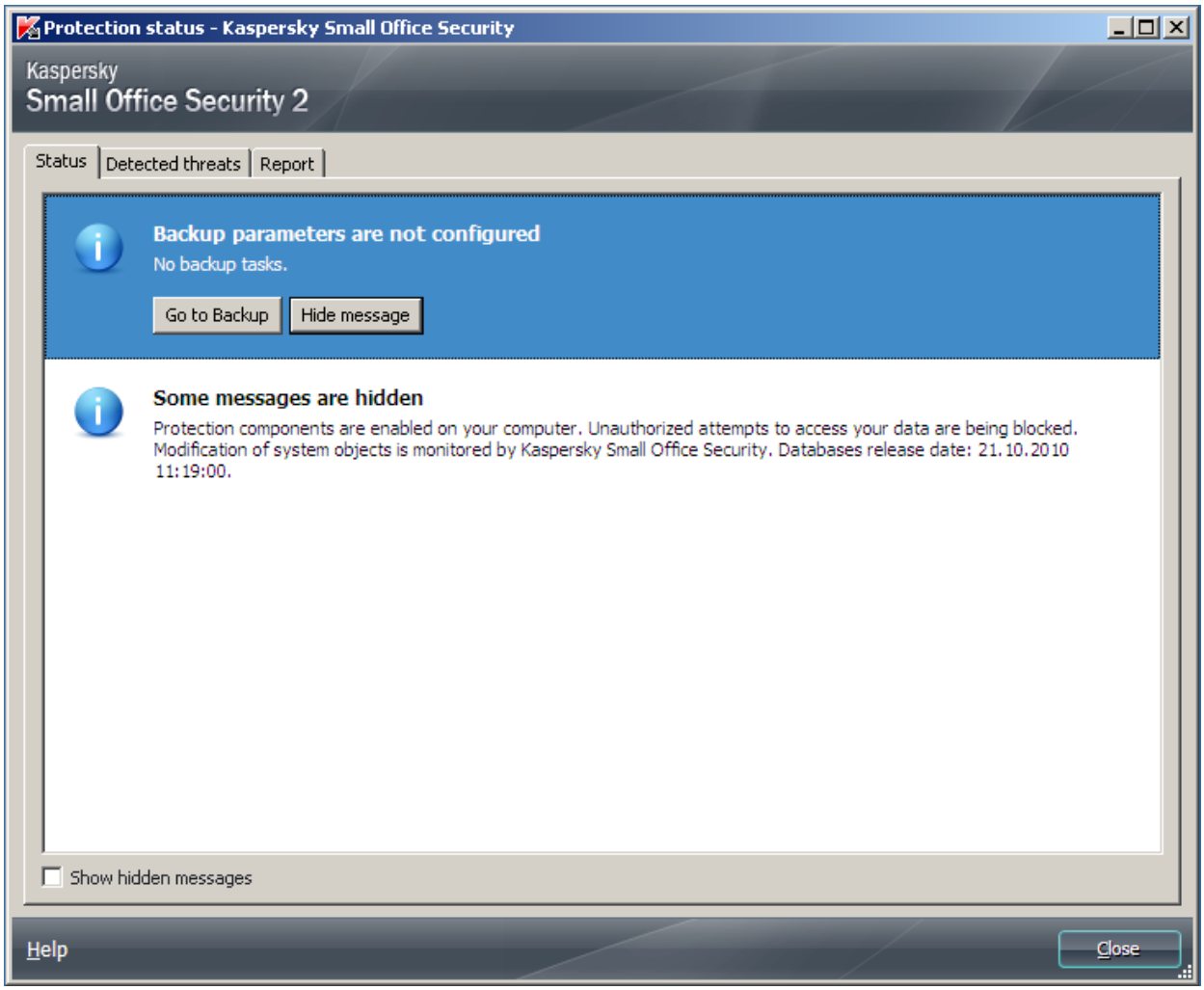
Protection status - Kaspersky Small Office Security
Kaspersky
Small Office Security 2
Status
Detected threats
Report
Backup parameters are not configured
No backup tasks.
Go to Backup
Hide message
Some messages are hidden
Protection components are enabled on your computer. Unauthorized attempts to access your data are being blocked. Modification of system objects is monitored by Kaspersky Small Office Security. Databases release date: 21.10.2010 11:19:00.
Show hidden messages
Help
Close

*Figure 7. The **Protection status** window*

The **Status** tab of the **Protection state** window lists the protection-related problems including those caused by deviations from the normal product operation mode (e.g., outdated databases). To address the issues, the product offers the following options as further steps:

- Remove immediately. Clicking the corresponding buttons will take you to the appropriate problem solution. This is the recommended action.

- Postpone removal. If, for whatever reason, immediate removal of the problem is not possible, you can postpone this action and return to it later. To do this, click the **Hide message** button.

  Note that postponing the removal is not available for serious problems. Such problems include, for example, malicious objects that were not disinfected, crashes of one or several components, or corruption of program files.

To display the notifications hidden earlier in the common list, check the **Show hidden messages** box, which appears in the bottom part of the tab when there are hidden messages.

You can use the **Detected threats** tab to view the list of detected malware and riskware and select an action to take on those objects (e.g., move to Quarantine). To select an operation, use the controls above the list and the context menu for the listed records.

On the **Report** tab, you can view the application activity reports (see section "How to view the report on computer protection" on page 60).

You can analyze the level of protection of an office network from the administrator's workplace using Management Console (see section "How to check the protection status of an office computer network remotely" on page 47).

ENABLING / DISABLING COMPUTER PROTECTION

By default, Kaspersky Small Office Security is launched when the operating system loads and protects your computer until it is switched off. All protection components are running.

You can fully or partially disable the protection provided by Kaspersky Small Office Security.

The Kaspersky Lab specialists strongly recommend that you **do not disable protection**, since this could lead to an infection of your computer and data loss.

When protection is disabled, all its components become inactive. This is indicated as follows:

- inactive (grey) icon of Kaspersky Small Office Security (see section "Taskbar notification area icon" on page 29) in the taskbar notification area;

- red color of the security indicator.

In this case, protection is seen in the context of the protection components. Disabling or pausing protection components does not effect the performance of virus scan tasks and Kaspersky Small Office Security updates.

To disable protection completely:

1. Open the main application window and click the **Settings** link in the top part.

2. In the window that opens, in the **Protection Center** section, select the **General Settings** subsection.

3. Uncheck the **Enable protection** box.

To turn on / off a separate protection component, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Protection Center** section.

3. In the right part of the window, click the button with the name of the category of protected objects, to which the protection component belongs.

4. In the **Protection components** window that opens, enable / disable the required protection component by clicking the status icon to the right from the component name.

PAUSING PROTECTION

Pausing protection means temporarily disabling all protection components for a certain period of time.

As a result of temporarily disabling protection, all protection components will be paused. This is indicated by:

- inactive (grey) application icon (see section "Taskbar notification area icon" on page 29) in the taskbar notification area;

- red color of the status icon and panel of the computer protection window.

If network connections were established at the same time as protection was paused, a notification about termination of such connections is displayed.

To pause the protection of your computer:

1. In the application icon context menu (see section "Context menu" on page 30) select the **Pause protection** item.

2. In the **Pause protection** window that will open, select the time interval after which the protection should be resumed:

   - **Pause for the next <time interval>** – protection will be enabled in a specified amount of time. Use the dropdown menu to select the time interval value.

   - **Pause until reboot** – protection will be enabled after application restart or after the system restart (provided that Kaspersky Small Office Security is set to start automatically on startup).

   - **Pause** – protection will be enabled only after you start it manually. To enable protection, select the **Resume protection** item from the application icon context menu.

USING INTERACTIVE PROTECTION MODE

Kaspersky Small Office Security uses two modes to interact with the user:

- *Interactive protection mode*. Kaspersky Small Office Security notifies the user of all hazardous and suspicious events. In this mode, the user independently decides whether to allow or block actions.

- *Automatic protection mode*. Kaspersky Small Office Security will automatically apply actions recommended by Kaspersky Lab in response to dangerous events.

To select protection mode:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **General Settings** subsection.

4. In the right part of the **Interactive protection** section, check or uncheck the boxes depending on the selected protection mode:

   - to enable interactive protection mode, uncheck the **Select action automatically**;
   - to enable automatic protection mode, check the **Select action automatically**.

   If you do not want Kaspersky Small Office Security to delete suspicious objects when running in automatic mode, check the **Do not delete suspicious objects** box.

RESOLVING TYPICAL TASKS

This section contains instructions on the basic tasks encountered by most users when working with the application.

IN THIS SECTION:

How to activate the application 41

How to purchase or renew a license 42

What to do when the application's notifications appear 43

How to update application databases and modules 43

How to scan critical areas of your computer for viruses 43

How to scan a file, folder, disk, or another object for viruses 44

How to perform full scan of your computer for viruses 46

Scanning computer for vulnerabilities 46

How to check the protection status of an office computer network remotely 47

How to protect your personal data against theft 47

What to do if you suspect an object of being infected with a virus 52

How to restore an object that has been deleted or disinfected by the application 52

What to do if you suspect your computer of being infected 53

How to create backup copies of your data 54

How to restrict access to Kaspersky Small Office Security settings 56

How to restrict computer and internet usage for different users 56

How to create and use Rescue Disk 57

What to do with a large number of spam messages 59

How to view the report on computer protection 60

How to restore application default settings 61

How to transfer application settings to another computer 61

HOW TO ACTIVATE THE APPLICATION

Activation is the procedure of activating a license that allows you to use a fully functional version of the application until the license expires.

If you have not activated the application during installation, you can do so later. You will be reminded about the need to activate the application by Kaspersky Small Office Security messages appearing in the taskbar notification area.

To run the Kaspersky Small Office Security activation wizard, perform one of the following:

- Click the **Please activate the application** link in the Kaspersky Small Office Security notice window appearing in the system tray.
- Click the **License** link in the bottom part of the main application window. In the **License management** window that opens, click the **Activate the application with a new license** button.

Let us review the steps of the Wizard in more detail.

Step 1. Selection of the license type and entry of the activation code

Make sure you have selected **Activate commercial version** in the Activation Wizard window, enter the activation code in the corresponding field, and click the **Next** button.

Step 2. Requesting for activation

At this step, the Wizard sends a request to the activation server to obtain permission for activation of the commercial version of the application. If the request is sent successfully, the Wizard automatically proceeds to the next step.

Step 3. Closing the Wizard

This window displays information on the activation results: type of license used and license expiry date.

Click the **Finish** button to close the Wizard.

HOW TO PURCHASE OR RENEW A LICENSE

If you have installed Kaspersky Small Office Security without a license, you can purchase one after installation. When your license expires, you can renew it. You will receive an activation code that you should use to activate the application (see section "How to activate the application" on page 41).

To purchase a license:

1. Open the main application window.
2. Click the **Purchase license** button in the bottom part of the window.

   The eStore web page opens where you can purchase a license.

To renew a license:

1. Open the main application window and click the **License** link in the bottom part of the main window.

   The **License management** window opens.
2. Click the **Renew license** button.

   The license renewal center web page opens where you can renew your license.

WHAT TO DO WHEN THE APPLICATION'S NOTIFICATIONS APPEAR

Notifications that appear in the taskbar notification area inform you of events occurring in the application's operation and requiring your attention. Depending on how critical the event is, you may receive the following types of notification:

- Critical notifications – inform you of events of critical importance from the viewpoint of computer security: for example, detection of a malicious object or dangerous activity in the system. Notification windows and pop-up messages of this type are red-colored.
- Important notifications – inform you of events which are potentially important from the viewpoint of computer security: for example, detection of a potentially infected object or suspicious activity in the system. Notification windows and pop-up messages of this type are yellow-colored.
- Informational messages – inform you of events that are non-critical from the viewpoint of security. Notification windows and pop-up messages of this type are green-colored.

If such a notification is displayed on the screen, you should select one of the suggested options. By default, the optimum option is the one recommended by Kaspersky Lab experts.

HOW TO UPDATE APPLICATION DATABASES AND MODULES

By default, Kaspersky Small Office Security automatically checks for updates on the Kaspersky Lab update servers. If the server contains new updates, Kaspersky Small Office Security downloads and installs them in the background mode. You can start a Kaspersky Small Office Security update at any time.

To download updates from Kaspersky Lab servers, you should have an established Internet connection.

To keep your computer's protection up to date, you are advised to update Kaspersky Small Office Security immediately after the installation.

To start the update from the context menu,

select **Update** from the context menu of the application icon.

To start update from the main application window:

1. Open the main application window.
2. Select the **Update Center** section in the left part of the window.
3. In the right part of the window, click the **Perform update** button.

HOW TO SCAN CRITICAL AREAS OF YOUR COMPUTER FOR VIRUSES

Quick Scan consists of scanning the objects which are loaded at startup of the operating system, scanning the system memory, boot sectors of the disk drive, and the objects that have been added by the user. After Kaspersky Small Office Security has been installed, it automatically performs a quick scan of your computer.

You can start the Quick Scan task using one of the following methods:

- using the shortcut created earlier (see page 71);
- from the main application window (see section "Kaspersky Small Office Security main window" on page 31).

To start the Quick Scan task using a shortcut:

1. Open the Microsoft Windows Explorer window and go to the folder where you have created the shortcut.
2. Double-click the shortcut to start the scan.

To start the Quick Scan task from the main application window:

1. Open the main application window.
2. In the left part of the window, select the **Scan** section.
3. In the right part of the window, click the **Start Quick Scan** button.

   Information about the scan in progress is displayed:

   - in the **Scan** section in the **Stop Quick Scan** section;
   - in the **Quick Scan** window that opens by clicking the **Finish** link in the **Stop Quick Scan** section;
   - in the application icon context menu (see page 30).

To stop the quick scan:

1. Open the main application window.
2. In the left part of the window, select the **Scan** section.
3. In the right part of the window, click the **Stop Quick Scan** button.

HOW TO SCAN A FILE, FOLDER, DISK, OR ANOTHER OBJECT FOR VIRUSES

You can use the following methods to scan an object for viruses:

- using the context menu of the object;
- from the main application window (see section "Kaspersky Small Office Security main window" on page 31).

To start a virus scan task from the object context menu:

1. Open the Microsoft Windows Explorer and go to the folder which contains the object to be scanned.

2. Right-click to open the context menu of the object (see figure below) and select **Scan for Viruses**.

   The process and the results of the task will be displayed in the **Virus Scan** window that opens.

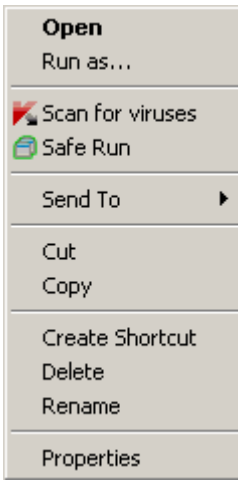

Figure 8. Context menu of an object in Microsoft Windows

To start scanning an object from the main application window:

1. Open the main application window.
2. In the left part of the window, select the **Scan** section.
3. In the right part of the window in the **Start Objects Scan** section, click the **Add** link.
4. In the **Select object to scan** window, specify the location of the object that you to scan for viruses.
5. In the **Start Objects Scan** section, select the checkboxes for the objects that you want to scan.
6. Click the **Start Objects Scan** button.

   Information about the scan in progress is displayed:

   - in the **Scan** section in the **Stop Objects Scan** section;
   - in the **Objects Scan** window that opens by clicking the **Finish** link in the **Stop Objects Scan** section;
   - in the application icon context menu (see page 30).

To stop objects scan:

1. Open the main application window.
2. In the left part of the window, select the **Scan** section.
3. In the right part of the window, click the **Stop Objects Scan** button.

HOW TO PERFORM FULL SCAN OF YOUR COMPUTER FOR VIRUSES

You can start the Full Scan task using one of the following methods:

- using the shortcut created earlier (see page 71);
- from the main application window (see section "Kaspersky Small Office Security main window" on page 31).

To start the Full Scan task using a shortcut:

1. Open the Microsoft Windows Explorer window and go to the folder where you have created the shortcut.
2. Double-click the shortcut to start the scan.

To start the Full Scan task from the main application window:

1. Open the main application window.
2. In the left part of the window, select the **Scan** section.
3. In the right part of the window, click the **Run Full Scan** button.

SCANNING COMPUTER FOR VULNERABILITIES

Vulnerabilities are unprotected portions of software code which intruders may deliberately use for their purposes, for example, to copy data used in unprotected applications. Scanning your computer for vulnerabilities helps you to reveal any such weak points in your computer. You are advised to remove the detected vulnerabilities.

You can use the following methods to scan the system for vulnerabilities:

- from the main application window (see section "Kaspersky Small Office Security main window" on page 31);
- using the shortcut created earlier.

To start the task using a shortcut:

1. Open the Microsoft Windows Explorer window and go to the folder where you have created the shortcut.
2. Double-click the shortcut to start scanning the system for vulnerabilities.

   Progress of the task will be displayed in the **Vulnerability Scan** window that opens.

To start the task from the main application window:

1. Open the main application window.
2. In the left part of the window, select the **Scan** section.
3. In the right part of the window, click the **Open Vulnerability Scan window** button.
4. In the window that opens, click the **Start Vulnerability Scan** button.

   Progress of the task will be displayed in the **Vulnerability Scan** window. Vulnerabilities that have been found will be displayed on the **System vulnerabilities** and **Vulnerable applications** tabs.

HOW TO CHECK THE PROTECTION STATUS OF AN OFFICE COMPUTER NETWORK REMOTELY

The Management Console functions are designed to control Kaspersky Small Office Security remotely from the administrator's workplace when installed on office network computers (see page 165).

You can analyze the overall level of protection of an office network or view a list of problems on an individual computer in the network and fix some of them remotely.

To obtain detailed information about problems in the network protection and eliminate them, please do the following:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console Configuration Wizard** button.

   This launches the Management Console Configuration Wizard. Let us take a closer look at the wizard's steps:

   a. Enter or set the administrator password in the **Password protection** window.

   b. Select a network subject to remote control in the **Network scan** window.

   c. Select the update mode for anti-virus databases in the **Update source** window.

   d. Confirm the settings you have selected in the **Summary** window.

   At further startups, you will need to enter the administrator password.
4. In the **Management Center** section of the main application window, click the **Management Console** button.
5. In the **Management Console** window that opens, click the status icon or the panel on which it is located.

   In the **Network protection status** window that opens, current problems are displayed.

To obtain the list of problems on a computer in the office network:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console** button.
4. In the left part of the **Management Console** window that opens, select the computer for which you want to view the list of problems, and go to the **Information** section.
5. In the right part of the window, select the **Problems list** item.
6. In the **General Protection Status** window that opens, current problems encountered on the selected computer are displayed.

HOW TO PROTECT YOUR PERSONAL DATA AGAINST THEFT

With Kaspersky Small Office Security, you can protect your personal data against theft; this includes items such as:

- passwords, usernames, and other registration data;

- account numbers and bank cards;
- confidential data.

Kaspersky Small Office Security includes components and tools that allow you to protect your personal data against theft attempts committed by hackers using methods such as phishing and the interception of data entered via the keyboard.

Protection against phishing is ensured by Anti-Phishing implemented in the Web Anti-Virus, Anti-Spam, and IM Anti-Virus components (only in Kaspersky Small Office Security 2 for Personal Computer).

Protection against the interception of data entered at the keyboard is ensured by the use of Virtual Keyboard and Password Manager (only in Kaspersky Small Office Security 2 for Personal Computer).

Protection of data against unauthorized access is ensured by the use of Data Encryption.

IN THIS SECTION:

Protection against phishing 48

Virtual Keyboard 49

Password Manager 49

Data Encryption 50

PROTECTION AGAINST PHISHING

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Phishing is a type of online fraud that involves tricking users into disclosing their credit card numbers, PIN codes and other privacy data with the objective of stealing funds.

Phishing often targets online banking users. Criminals create an exact copy of the website of a chosen bank and send emails to customers on behalf of this bank. They claim that a malfunction or replacement of online banking system software has resulted in the loss of user details, necessitating the user to confirm or modify such details on the bank's website. Users click the link that takes them to the fake website and enter their details, which then end up in the hands of criminals.

Protection against phishing is ensured by Anti-Phishing implemented in the Web Anti-Virus, Anti-Spam, and IM Anti-Virus components. Enable these components to ensure comprehensive protection against phishing.

To enable components providing protection against phishing:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. In the right part of the window, check the **Enable Web Anti-Virus** box.
5. Repeat steps 3 and 4 for the **Anti-Spam** and **IM Anti-Virus** components.

   The components that include Anti-Phishing will be enabled.

VIRTUAL KEYBOARD

When working on your computer, there are occasions when entering of your personal data, or username and password are required. For instance, when registering on Internet sites, using online stores etc.

There is a risk that this personal information is intercepted using hardware keyboard interceptors or keyloggers, which are programs that register keystrokes.

The Virtual Keyboard tool prevents the interception of data entered via the keyboard.

Virtual Keyboard cannot protect your personal data if the website, that required entering such data, has been hacked, since in this case the information will be obtained directly by the intruders.

Many of the applications classified as spyware have the function of making screenshots which are then transferred to an intruder for further analysis and for stealing the user's personal data. Virtual Keyboard prevents the personal data being entered, from being intercepted with the use of screenshots.

The Virtual Keyboard only prevents the interception of privacy data when working with Microsoft Internet Explorer and Mozilla Firefox browsers.

To start using Virtual Keyboard:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. Click the **Virtual Keyboard** button in the right part of the window.
4. Enter the required data by pressing the buttons on the virtual keyboard. Make sure that data is entered in the correct field. When you press function keys (**SHIFT**, **ALT**, **CTRL**) on the virtual keyboard, that particular mode will be fixed: for example, when you press **SHIFT** all symbols will be entered in the upper case. To exit the special mode, press the same functional key again.

You can switch the language for the virtual keyboard using the key combination **CTRL** + right-clicking **SHIFT**, or **CTRL** +right-clicking **ALT**, depending on the settings selected.

PASSWORD MANAGER

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Password Manager makes it possible to store different personal data (for example, user names, passwords, addresses, phone and credit card numbers).

All information is stored in encrypted form in the Password Database, access to which is protected by a Master Password. Password Manager sticks passwords and accounts to Microsoft Windows applications and web pages for which they are used. After launching a web page or application, Password Manager automatically enters the password, user name and other personal data. Thus, you need not remember all the passwords, you only need to remember one password.

To use Password Manager to automatically fill out the authorization form, do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Password Manager** button.

4. Click the **Start Password Manager** button.

   This starts the Password Manager Configuration Wizard. Let us take a closer look at the wizard's steps:

   a. Create a master password to protect your password database in the **Master Password** window.

   b. Select an authorization method to access your password database in the **Access control** window.

   c. In the **Locking timeout** window, set the time after which Password Manager will be automatically blocked.

5. On finishing the Password Manager Configuration Wizard, you are asked to type in the master password, after which the **Password Manager** main window becomes available.

6. In the **Password Manager** main window, click the **Add Password** button.

7. In the Account Creation Wizard that opens, select the type of account (Web Account, Application Account or expert mode):

   - If you have selected an Internet account or an application account, click the **Next** button.

     At the next step in the Account Creation Wizard, specify the website or application that the account is to be used for, and click the **Next** button.

   - If you have selected the advanced mode, click the **Next** button.

8. At the next step in the Account Creation Wizard, specify the account settings:

   - In the top part of the **Account Name** field, enter or edit the name of the new account.

   - Under the tab **Login information**, enter the user name (login) and password.

     The user name can consist of one or several words. To specify key words (see page 179) for the user name, click .

     To copy a user name / password to the clipboard, click the button.

     To copy a user name from another account, follow the **Use shared Login from another Account** link.

     To create a password automatically, open the Password Generator window by clicking the **Generate password** link (see page 203).

   - Under the **Links** tab, specify the path to the program / web page, and specify the account's settings.

   - On the **Manual form edit** tab, modify the settings for populating other fields of the web page, if necessary.

   - If necessary, under the **Comments** tab, enter some explanatory text for the account. To display comments in a notification after activating the account, check the **Show comments in the notification** box.

9. Click the **Add Account** button.

10. Run the application / web page for which the account was created.

    The authorization form will be filled automatically using data from the account.

DATA ENCRYPTION

To protect confidential information from unauthorized access, you are recommended to store it in encrypted form in a special container.

Create a container, save the data in it, and then encrypt the data. A password will now be required to access the data in the container.

To create an encrypted container, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Data Encryption** button.
4. In the window that opens, click the **Create container** button.

   The Encrypted Container Creation Wizard will be started.
5. In the Encrypted Container Creation Wizard, specify the settings of the container to be created:

   a. In the **General settings** window, type in the name of the container, its size and the password to access data in the container.

   b. In the **Location** window, specify the location of the container file.

   c. In the **Summary** window, select the letter of the virtual disk to connect the container, specify any additional settings, and click the **Finish** button to confirm these settings to create the container.

To write data to the container:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Data Encryption** button.
4. In the window that opens, select the container in the list and click the **Open** button.

   The container opens in the Microsoft Windows Explorer window.
5. Place in it the data you want to encrypt.
6. In the **Data Encryption** window, click the **Encrypt data** button.

To gain access to the data in the container, do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Data Encryption** button.
4. In the window that opens, select the container in the list and click the **Encrypt data** button.
5. In the window that will open, enter the password to obtain access to the container.
6. In the **Data Encryption** window, click the **Open** button.

WHAT TO DO IF YOU SUSPECT AN OBJECT OF BEING INFECTED WITH A VIRUS

If you suspect an object of being infected, first scan it using Kaspersky Small Office Security (see section "How to scan a file, folder, disk, or another object for viruses" on page 44).

After the scan, if the application reports that the object is not infected, but you think that it is, you can do the following:

- Move the object to *Quarantine*. Objects moved to Quarantine do not pose any threat to your computer. After the databases are updated, Kaspersky Small Office Security will probably be able to clearly identify and remove the threat.
- Send the object to *Virus Lab*. Virus Lab specialists scan the object. If it turns out to be infected with a virus, they immediately add the description of the new virus in the databases that will be downloaded by the application with an update (see section "How to update application databases and modules" on page 43).

You can move an object to Quarantine using one of the two methods:

- using the **Move to Quarantine** link in the **Protection state** window;
- using the context menu of the object.

*To move an object to Quarantine from the **Protection state** window:*

1. Open the main application window.
2. In the top part of the window, use the **Quarantine** link to open the **Protection status** window.
3. On the **Detected threats** tab, follow the **Quarantine** link.
4. In the window that opens, select the object that you want to move to Quarantine.

To move an object to Quarantine using the context menu:

1. Open the Microsoft Windows Explorer window and go to the folder that contains the object that you want to move to Quarantine.
2. Right-click to open the context menu of the object and select **Move to Quarantine**.

To send an object to the Virus Lab:

1. Go to the Virus Lab request page (http://support.kaspersky.com/virlab/helpdesk.html).
2. Follow the instructions on this page to send your request.

HOW TO RESTORE AN OBJECT THAT HAS BEEN DELETED OR DISINFECTED BY THE APPLICATION

Kaspersky Lab recommends that you avoid restoring deleted and disinfected objects since they may pose a threat to your computer.

If you want to restore a deleted or disinfected object, you can use a backup copy of it which was created by the application when scanning the object.

To restore an object that has been deleted or disinfected by the application:

1. Open the main application window.
2. In the top part of the window, use the **Quarantine** link to open the **Protection status** window.
3. On the **Detected threats** tab, in the dropdown list located over the list of threats, select **Neutralized**.

   The list of disinfected and deleted objects is displayed on the tab. Objects are grouped according to their status. To display the list of objects in a group, click the **+** icon located to the left of the group header.
4. Right-click to open the context menu of the object that you want to restore, and select **Restore**.

WHAT TO DO IF YOU SUSPECT YOUR COMPUTER OF BEING INFECTED

If you suspect that your computer has been infected, use the *System Restore Wizard* to neutralize the consequences of malicious activity in the system. Kaspersky Lab recommends that you run the Wizard after the computer has been disinfected to make sure that all threats and damage caused by infections have been fixed.

The Wizard checks whether there are any changes to the system, such as the following: access to the network being blocked, known file format extensions have been changed, the toolbar is locked, etc. Such damage can have various causes. The latter may include the activity of malicious programs, incorrect system configuration, system failures or even incorrect operation of system optimization applications.

After the review is complete, the Wizard analyzes the information to evaluate whether there is system damage which requires immediate attention. Based on the review, a list of actions necessary to eliminate the problems is generated. The Wizard groups these actions by category based on the severity of the problems detected.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the System Restore Wizard:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Additional Tools** button.
4. In the **Additional Tools** window that opens, click the **System Restore** button.

The Wizard steps in detail.

Step 1. Starting system restore

Make sure that the Wizard option to **Search for problems caused by malware activity** is selected and click the **Next** button.

Step 2. Problem search

The Wizard will search for problems and damage, which should be fixed. Once the search is complete, the Wizard will automatically proceed to the next step.

Step 3. Selecting troubleshooting actions

All damage found during the previous step is grouped on the basis of the type of danger it poses. For each damage group, Kaspersky Lab recommends a sequence of actions to repair the damage. There are three groups of actions:

- *Strongly recommended actions* eliminate problems posing a serious security threat. You are advised to perform all actions in this group.
- *Recommended actions* eliminate problems presenting a potential threat. You are also advised to perform all actions in this group.
- *Additional actions* repair system damage which does not pose a current threat, but may pose a danger to the computer's security in the future.

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

It is strongly recommended not to uncheck the boxes selected by default because doing so will leave your computer vulnerable to threats.

Having defined the set of actions, which the Wizard will perform, click the **Next** button.

Step 4. Problems elimination

The Wizard will perform the actions selected during the previous step. The elimination of problems may take some time. Once the troubleshooting is complete, the Wizard will automatically proceed to the next step.

Step 5. Closing the Wizard

Click the **Finish** button to close the Wizard.

HOW TO CREATE BACKUP COPIES OF YOUR DATA

The most common way to protect important data from being lost is to regularly back it up. Kaspersky Small Office Security can automatically make regular scheduled backup copies of selected data in the specified storage area. You can also make one-off backup copies.

Before you can start working, you should create a backup storage on the selected drive. The backup copies of required files will be created in this storage. After that, you can configure backup tasks (choose files, for which backup tasks should be created, configure startup schedule and other backup conditions).

To create a backup storage area, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Storage** section and click the **Create** button.

5. Backup Storage Creation Wizard will be launched. Let us take a closer look at the wizard's steps:

   a. In the left part of the **Drive** window, select the type of data storage medium which will be used as a backup storage.

   > To ensure data security, we recommend that you create backup storages on removable disk drives.

   b. In the **Protection** window, set a password to protect data against unauthorized access (if necessary).

   c. In the **File versions** window, set a limit on the number of file versions which may coexist within the storage, and specify the time interval for storing backup copies (if necessary).

   d. In the **Summary** window, enter the name for the new storage and confirm the storage creation with the settings you have specified.

To back up objects, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Backup** section and click the **Create** button.
5. The Backup Task Creation Wizard will be launched. Let us take a closer look at the wizard's steps:

   a. In the **Content** window, select the objects for which backup copies will be created.

   b. In the **Storage** window, select the storage in which backup copies of files will be created.

   c. In the **Schedule** window, specify the conditions for running the task.

   > If you want to make a one-off backup copy, uncheck the **Run by schedule** box.

   d. Enter the name of the new task and click the **Finish** button in the **Summary** window.

To restore the data of the backup copy, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Restore** section.
5. Select the storage where the required backup copies are located and click the **Restore** button.
6. In the top part of the **Restore data from storage** window, select an archive (set of data saved during a task) in the dropdown list.
7. Select the files that need to be restored. To do this, check the boxes next to the required files in the list. To select all files, click the **Select all** button in the bottom part of the list. Click the **Restore** button in the top part of the window.
8. In the **Restore** window that opens, select the location to save restored files and the condition of saving if files' names coincide. Click the **Restore** button.

   The most recent versions of the selected files will be restored.

HOW TO RESTRICT ACCESS TO KASPERSKY SMALL OFFICE SECURITY SETTINGS

A computer may be used by several users with various levels of computer literacy. Unrestricted access to Kaspersky Small Office Security and its settings granted to users may lead to reduced level of computer protection.

To restrict access to the application, you can set a password and specify which actions should require entering the password:

- changing application settings;
- Backup management;
- Web Policy Management (only in Kaspersky Small Office Security 2 for Personal Computer);
- remote management of network security;
- closing the application.

To protect access to Kaspersky Small Office Security with a password, please do the following:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Administrator Password** section, select the **General Settings** subsection.
4. In the right part of the window, under **Password protection**, check the **Enable password protection** box and fill in the **New password** and **Confirm new password** fields.
5. In the **Password scope** section set a scope within which access will be restricted. Now whenever any user on your computer attempts to perform the actions you have selected, Kaspersky Small Office Security will always request the password.

To change the password to access Kaspersky Small Office Security, do the following:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Administrator Password** section, select the **General Settings** subsection.
4. In the right part of the window, under **Password protection**, fill in the **Old password**, **New password** and **Confirm password** fields.

HOW TO RESTRICT COMPUTER AND INTERNET USAGE FOR DIFFERENT USERS

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Immediately after the installation of Kaspersky Small Office Security, there are no restrictions for computer users. To ensure compliance with the company's rules and regulations regarding employee use of the computer and the internet, configure the Web Policy Management settings for all users of the computer.

If you have not enabled password protection when installing the application, at the first startup of Web Policy Management you are recommended to set a password for protection from unauthorized modification of the Control settings. After that, you can enable Web Policy Management and configure restrictions for computer and Internet usage for all accounts on the computer.

To configure Web Policy Management for an account, please do the following:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. Click the **Enable Web Policy Management** button in the right part of the window..
4. In the list of accounts, select the account whose control settings need to be configured and click the **Configure policies** button.
5. In the left part of the window that opens, select the type of restriction and configure the control settings in the right part of the window.

HOW TO CREATE AND USE RESCUE DISK

We recommend that you create Rescue Disk after you have installed and configured Kaspersky Small Office Security, scanned your computer, and made sure that it was not infected. You will further be able to use Rescue Disk for scanning and disinfecting infected computers that cannot be disinfected using other methods (e.g., with anti-virus applications).

IN THIS SECTION:

Create Rescue Disk 57

Starting the computer from the Rescue Disk 59

CREATE RESCUE DISK

Creating the Rescue Disk means the creation of a disk image (ISO file) with up-to-date anti-virus databases and configuration files.

The source disk image serving as a base for new file creation can be downloaded from the Kaspersky Lab server or copied from a local source.

You can create Rescue Disk using the *Rescue Disk Creation Wizard*. The rescuecd.iso file created by the Wizard is saved on your computer's hard drive:

- in Microsoft Windows XP – in the following folder: Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP9\Data\Rdisk\;
- in Microsoft Windows Vista and Microsoft Windows 7 operating systems – in the following folder: ProgramData\Kaspersky Lab\AVP9\Data\Rdisk\.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the Rescue Disk Creation Wizard:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Additional Tools** button.

4. In the **Additional Tools** window that opens, click the **Rescue Disk** button.

The Wizard steps in detail.

Step 1. Starting the Wizard. Searching for an existing disk image

The first window of the Wizard contains information about the Rescue Disk that will be created by the Wizard.

If the Wizard detects an existing Rescue Disk ISO file in the dedicated folder (see above), the **Use existing ISO image** box will be displayed in the first window of the Wizard. Check the box to use the detected file as original ISO image and go directly to the **Updating disk image** step (see below). Uncheck this box if you do not want to use the disk image that has been found, and the Wizard proceeds to the **Select disk image source** window.

Step 2. Select disk image source

At this step, you should select the image file source from the list of options:

- Select **Copy ISO image from local or network drive** if you already have a Rescue Disk or an image prepared for it and stored on your computer or on a local network resource.

- Select the **Download disk image from Kaspersky Lab server** option if you do not have an image file, and you want to download it from the Kaspersky Lab server (file size is about 100 MB).

Step 3. Copying (downloading) disk image

If you have selected the option to copy the image from a local source at the previous step (**Copy ISO image from local or network drive**), you should specify the path to the ISO file at this current step. To do this, click the **Browse** button. After you have specified the path to the file, click the **Next** button. The disk image copying progress is displayed in the Wizard window.

If you have selected **Download ISO image from Kaspersky Lab server**, the disk image downloading progress is displayed immediately.

When copying or downloading the ISO image is complete, the Wizard automatically proceeds to the next step.

Step 4. Updating image file

File update procedure includes:

- update of anti-virus databases;

- update of configuration files.

Configuration files determine the possibility of starting the computer from a CD / DVD written using a rescue disk image provided by the wizard.

When updating anti-virus databases, those distributed at the last update of Kaspersky Small Office Security are used. If the databases are obsolete, it is recommended to update and restart the Rescue Disk Creation Wizard.

To begin updating the ISO file, click the **Next** button. The updating progress will be displayed in the Wizard window.

Step 5. Closing the Wizard

To complete the Wizard, click the **Finish** button. You can save the newly created iso file on CD or DVD and then use it to boot the computer.

STARTING THE COMPUTER FROM THE RESCUE DISK

If the operating system cannot be started as a result of a virus attack, use the Rescue Disk.

To boot the operating system, you should use a CD or DVD disc with the Rescue Disk image (.iso) file recorded on it.

To boot your computer from the Rescue Disk:

1. In BIOS settings enable start up from a CD / DVD disc (for detailed information please refer to the documentation for your computer's motherboard).
2. Insert the CD / DVD disc with the Rescue Disk image into the CD / DVD drive of an infected computer.
3. Restart your computer.

For detailed information about the use of the Rescue Disk, please refer to the Kaspersky Rescue Disk User Guide.

WHAT TO DO WITH A LARGE NUMBER OF SPAM MESSAGES

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

If you receive large quantities of unsolicited mail (spam), enable the Anti-Spam component and set the recommended security level. Then train the component using the *Training Wizard*. Correct spam recognition requires training using at least 50 samples of useful messages and 50 samples of unwanted mail.

To enable Anti-Spam and set the recommended security level:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. In the right part of the window, check the **Enable Anti-Spam** box.
5. In the **Security level** section, the security level should be set to **Recommended** by default.

   If the security level is set to **Low** or **Custom**, click the **Default level** button. The security level will automatically be set to **Recommended**.

To train Anti-Spam using the Training Wizard:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Train** button in the **Anti-Spam training** section within the right part of the window.

   The Training Wizard window opens.

The Wizard steps in detail.

Step 1. Starting the Wizard

Click the **Next** button to start the training.

Step 2. Selecting folders containing good mail

At this stage, you can specify folders which contain good mail. You should only select folders which you are absolutely sure contain good email messages.

Only Microsoft Office Outlook and Microsoft Outlook Express (Windows Mail) accounts are accessible.

Step 3. Selecting folders containing spam

At this stage you can specify folders containing unsolicited mail (spam). If you do not have such folders in your email client application, skip this step.

Only Microsoft Office Outlook and Microsoft Outlook Express (Windows Mail) accounts are accessible.

Step 4. Training Anti-Spam

At this stage, the Anti-Spam component is trained using the folders selected during the previous steps. The emails in those folders fill the Anti-Spam database. The senders of good mail are automatically added to the list of allowed senders.

Step 5. Saving the training results

At this stage of the Wizard, you must save the training results using one of the following methods:

- add training results into the existing Anti-Spam database (select **Add the results to an existing Anti-Spam database**);
- replace the current database with a database containing only the training results (select the option **Create new Anti-Spam database**).

Click the **Finish** button to close the Wizard.

HOW TO VIEW THE REPORT ON COMPUTER PROTECTION

Kaspersky Small Office Security creates operation reports for each component. Using a report, you can find out, for example, how many malicious objects (such as viruses and Trojan programs) have been detected and removed by the application during the specified period, how many times the application has been updated during the same period, how many spam messages have been detected, and many other characteristics.

To view the application operation report:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Small Office Security.

   The **Report** tab of the window that opens displays application operation reports in diagram format.

3. If you want to view a detailed application operation report (for example, a report representing the operation of each component), click the **Detailed report** button in the bottom part of the **Report** tab.

   The **Detailed report** window opens where data are represented in a table. For a convenient view of reports, you can select various entry sorting options.

HOW TO RESTORE APPLICATION DEFAULT SETTINGS

You can always return to the default or recommended Kaspersky Small Office Security settings. They are considered optimum, and are recommended by Kaspersky Lab. Application Configuration Wizard restores default settings.

In the window that opens, you will be asked to determine which settings and for which components should or should not be saved when restoring the recommended security level.

The list shows which components of Kaspersky Small Office Security have settings that differ from the default values, either because they have been modified by the user, or through accumulated training by Kaspersky Small Office Security (Firewall or Anti-Spam). If special settings have been created for any of the components, they will also be shown on the list.

Examples of special settings would be: white and black lists of phrases and addresses used by Anti-Spam, lists of trusted addresses and trusted ISP telephone numbers, exclusion rules created for application components, and Firewall's packet and application filtering rules.

These lists are created when working with Kaspersky Small Office Security with regard to individual tasks and security requirements. Creating them may take a long time, so you are advised to save them before restoring the application's default settings.

After you are finished with the Configuration Wizard, the **Recommended** security level will be set for all components, except for the settings that you have decided to keep customized when restoring. In addition, the settings that you have specified when working with the Wizard will also be applied.

To restore protection settings:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **General** subsection.
4. Click the **Restore** button in the right part of the window.
5. In the window that opens, click the **Next** button. This will run the Application Configuration Wizard. Follow its instructions.

HOW TO TRANSFER APPLICATION SETTINGS TO ANOTHER COMPUTER

Having configured the product, you can apply its settings in Kaspersky Small Office Security installed on another computer. Consequently, the application will be configured identically on both computers. This is a helpful feature when, for example, Kaspersky Small Office Security is installed on your home computer and in your office.

Application settings are stored in a special configuration file, which you can transfer to another computer. To do this:

1. Perform the *Export* procedure – save the application settings to a configuration file.

2. Move the file you have saved to another computer (for example, send it by email or use a removable data medium).

3. Perform the *Import* procedure – apply the settings from the configuration file to the application installed on another computer.

To export the current settings of Kaspersky Small Office Security:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **General Settings** section, select the **General** subsection.

4. Click the **Save** button in the right part of the window.

5. In the window that opens enter the name of the configuration file and the path where it should be saved.

To import the application's settings from a saved configuration file:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **General Settings** section, select the **General** subsection.

4. Click the **Load** button in the right part of the window.

5. In the window that opens, select a file from which you wish to import the Kaspersky Small Office Security settings.

ADVANCED APPLICATION SETTINGS

This section provides detailed information about each application component and describes the operation and configuration algorithms for each component.

IN THIS SECTION:

Scan 64

Update 72

File Anti-Virus 77

Mail Anti-Virus 83

Web Anti-Virus 89

IM Anti-Virus 95

Anti-Spam 96

Anti-Banner 113

Security Zone 116

Proactive Defense 124

Network protection 126

Trusted zone 137

Safe mode of applications execution 138

Quarantine and Backup 142

Backup 145

Web Policy Management 152

Data Encryption 161

Management Console 165

Password Manager 170

Performance and compatibility with other applications 206

Kaspersky Small Office Security self-defense 209

Application appearance 210

Additional Tools 212

Reports 218

Notifications 222

Participating in the Kaspersky Security Network 224

SCAN

Scanning the computer for viruses and vulnerabilities is one of the most important tasks in ensuring the computer's security. It is necessary to scan your computer for viruses on a regular basis in order to rule out the possibility of spreading malicious programs that have not been discovered by protection components, for example, because of a low security level set, or for other reasons.

Vulnerability scan performs the diagnostics of operating system and detects software features that can be used by intruders to spread malicious objects and obtain access to personal information.

The following sections contain detailed information about scan tasks features and configuration, security levels, scan methods, and scan technologies.

IN THIS SECTION:

Virus scan 64

Vulnerability Scan 71

VIRUS SCAN

Kaspersky Small Office Security comprises the following tasks to scan for viruses:

- **Custom Scan**. Objects, selected by the user, are scanned. Any object of the computer's file system can be scanned. Within this task you can configure the settings for scanning removable drives.
- **Full Scan**. A thorough scan of the entire system. The following objects are scanned by default: system memory, programs run on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Quick Scan**. Operating system startup objects are scanned.

It is not recommended to change the list of objects scanned by the Full and Quick Scan tasks.

Each scan task is performed in the specified area and can be started according to the schedule created. Besides, each scan task is characterized with a security level (combination of settings that impact the proportion between performance and security). By default, the mode of using records from application databases to search for threats is always enabled. You can also apply various scan methods and technologies (see page 68).

After the virus scan task starts, its progress is displayed under the name of the task in the **Scan** section of the main application window.

If a threat is detected, Kaspersky Small Office Security assigns one of the following statuses to the found object:

- malicious program (such as a *virus* or *Trojan*);
- *potentially infected* (suspicious) status if the scan cannot determine whether the object is infected or not. The file may contain a sequence of code appropriate for viruses, or modified code from a known virus.

The application displays a notification (see page222) about detected threat and performs the assigned action. You can change actions to be performed on detected threat.

If you work in automatic mode (see section "Using interactive protection mode" on page 39), Kaspersky Small Office Security will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**. If you work in interactive mode (see section "Using interactive protection mode" on page 39), Kaspersky Small Office Security displays a notification window, in which you will be able to choose one of the available actions.

Before attempting to disinfect or delete an infected object, Kaspersky Small Office Security creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable the automatic scan for quarantined objects after each update.

Information on the scan results and events, which have occurred during the execution of the task, is logged in a Kaspersky Small Office Security report.

IN THIS SECTION:

Changing and restoring security level 65

Creating the scan startup schedule 66

Creating a list of objects to scan 67

Selecting the scan method 67

Selecting the scan technology 68

Changing actions to be performed on detected objects 68

Running scan under a different user account 68

Changing the type of objects to scan 69

Scan of compound files 69

Scan optimization 70

Scanning removable drives on connection 71

Creating a task shortcut 71

CHANGING AND RESTORING SECURITY LEVEL

Depending on your current needs, you can select one of the preset security levels, or modify the scan settings manually.

When configuring scan task settings, you can always restore the recommended ones. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To change the defined security level, perform the following actions:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).

4. In the **Security level** section, set the required security level for the task selected, or click the **Settings** button to modify scan settings manually.

   If you modify the settings manually, the name of the security level will change to **Custom**.

To restore the default scan settings:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).
4. In the **Security level** section, click the **Default level** button for the task selected.

CREATING THE SCAN STARTUP SCHEDULE

You can create a schedule to automatically start virus scan tasks: specify task run frequency, start time (if necessary), and advanced settings.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the skipped task to start automatically as soon as it becomes possible. You can automatically pause the scan when a screensaver is inactive or the computer is unlocked. This functionality postpones the launch until the user has finished working on the computer. The scan will then not take up system resources during the work.

To modify a schedule for scan tasks:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, select the required task in the **Computer scan** (**Full Scan**, **Quick Scan**, **Objects Scan**, or **Vulnerability Scan**) section.
4. In the **Run mode** block, click the **Settings** button for the task selected.
5. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and configure the scan run mode.

To configure automatic launches of skipped tasks:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, select the required task in the **Computer scan** (**Full Scan**, **Quick Scan**, **Objects Scan**, or **Vulnerability Scan**) section.
4. In the **Run mode** block, click the **Settings** button for the task selected.
5. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and check the **Run skipped tasks** box.

To launch scans only when the computer is not being used:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, select the required task in the **Computer scan** (**Full Scan**, **Quick Scan**, **Objects Scan**, or **Vulnerability Scan**) section.

4. In the **Run mode** block, click the **Settings** button for the task selected.

5. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and check the **Pause scheduled scan when screensaver is inactive and computer is unlocked** box.

CREATING A LIST OF OBJECTS TO SCAN

Each virus scan task has its own default list of objects. These objects may include items in the computer's file system, such as logical drives and **email databases**, or other types of objects such as network drives. You can edit this list.

If the scan scope is empty, or it contains no selected objects, a scan task cannot be started.

To create a list of objects for an object scan task:

1. Open the main application window.

2. In the left part of the window, select the **Scan** section.

3. In the right part of the window, click the **Add** link to open the list of objects for scanning.

4. In the **Select object to scan** window that opens, select an object and click the **Add** button. Click the **OK** button after you have added all the objects you need. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

To create the list of objects for Quick Scan, Full Scan or Vulnerability Scan tasks:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, select the required task in the **Computer scan** (**Full Scan**, **Quick Scan**, or **Vulnerability Scan**) section.

4. In the **Objects to scan** section, click the **Settings** button for the task selected.

5. In the **Objects to scan** window that opens, use the **Add**, **Edit**, and **Delete** links to create a list. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

   Objects which appear on the list by default cannot be edited or deleted.

SELECTING THE SCAN METHOD

During virus scan, *signature analysis* is always used: Kaspersky Small Office Security compares the object found with the database records.

You can use the additional scan methods to increase the scan efficiency: *heuristic analysis* (analysis of the actions an object performs within the system) and *rootkit scan* (tools that can hide malicious programs in your operating system).

To specify which scan method to use:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).

4. In the **Run mode** block, click the **Settings** button for the task selected.

5. In the window that opens, on the **Additional** tab, in the **Scan methods** block, select the required values for the settings.

SELECTING THE SCAN TECHNOLOGY

In addition to the scan methods you can use special technologies, allowing you to increase the virus scan speed by excluding the files that have not been modified since they were last scanned.

To enable the object scan technologies:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).

4. In the **Run mode** block, click the **Settings** button for the task selected.

5. In the window that opens, on the **Additional** tab, in the **Scan technologies** block, select the required values for the settings.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If infected or potentially infected objects are detected, the application performs the specified action.

To change the action to be performed on detected objects:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).

4. In the **Action** block, specify the required action for the task selected.

RUNNING SCAN UNDER A DIFFERENT USER ACCOUNT

By default, the scan tasks are run under your system account. However, you may need to run task under a different user account. You can specify an account to be used by the application when performing a scan task.

To start the scan under a different user's account:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, select the required task in the **Computer scan** (**Full Scan**, **Quick Scan**, **Objects Scan**, or **Vulnerability Scan**) section.

4. In the **Run mode** block, click the **Settings** button for the task selected.

5. In the window that opens, on the **Run mode** tab, in the **User account** section, check the **Run task as** box. Specify the user name and password.

CHANGING THE TYPE OF OBJECTS TO SCAN

When specifying the type of objects to scan, you establish which file formats and sizes will be scanned for viruses when the selected scan task runs.

When selecting file types please remember the following:

- Probability of malicious code penetrating several file formats (such as .txt) and its further activation is quite low. At the same time, there are formats that contain or may contain an executable code (such as .exe, .dll, .doc). The risk of penetrating and activating malicious code in such files is quite high.

- The intruder can send a virus to your computer in an executable file renamed as txt file. If you have selected the scan of files by extension, such a file is skipped by the scan. If the scan of files by format is selected, then, regardless of the extension, File Anti-Virus will analyze the file header, and reveal that the file is an .exe file. Such a file would be thoroughly scanned for viruses.

To change the type of scanned objects:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).

4. In the **Security level** section, click the **Settings** button for the task selected.

5. In the window that opens, on the **Scope** tab, in the **File types** section, select the required option.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden in this way a compound file should be unpacked, which can significantly lower the scan speed.

For each type of compound file, you can select to scan either all files or only new ones. To make your selection, click the link next to the name of the object. It changes its value when you left-click it. If you select the scan new and changed files only scan mode (see page 70), you will not be able to select the links allowing you to scan all or new only files.

You can restrict the maximum size of the compound file being scanned. Compound files larger than the specified value will not be scanned.

To modify the list of scanned compound files:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).

4. In the **Security level** section, click the **Settings** button for the task selected.

5. In the window that opens, on the **Scope** tab, in the **Scan of compound files** section, select the required types of compound files to be scanned.

In order to set the maximum size of compound files to be scanned:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).
4. In the **Security level** section, click the **Settings** button for the task selected.
5. In the window that opens, on the **Scope** tab, in the **Scan of compound files** section, click the **Additional** button.
6. In the **Compound files** window that opens, check the **Do not unpack large compound files** box and specify the maximum file size.

When large files are extracted from archives, they will be scanned even if the **Do not unpack large compound files** box is checked.

SCAN OPTIMIZATION

You can shorten the scan time and speed up Kaspersky Small Office Security. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

You can also set a restriction on scan duration for an object. When the specified time interval expires, the object will be excluded from the current scan (except for archives and files comprised of several objects).

To scan only new and changed files:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).
4. In the **Security level** section, click the **Settings** button for the task selected.
5. In the window that opens, on the **Scope** tab, in the **Scan optimization** section, check the **Scan only new and changed files** box.

To set a restriction on scan duration:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, select the required task in the **Computer scan** section (**Full Scan**, **Quick Scan**, or **Objects Scan**).
4. In the **Security level** section, click the **Settings** button for the task selected.
5. In the window that opens, on the **Scope** tab, in the **Scan optimization** section, check the **Skip objects scanned longer than** box and specify the scan duration for a single file.

SCANNING REMOVABLE DRIVES ON CONNECTION

Nowadays, malicious objects using operating systems' vulnerabilities to replicate via networks and removable media have become increasingly widespread. Kaspersky Small Office Security allows to scan removable drives when connecting them to the computer.

To configure scanning of removable media at connection:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Scan** section, select the **General Settings** subsection.
4. In the right part of the window, in the **Scan removable drives on connection** block, select an action, and define the maximum size of a drive to scan in the field below, if necessary.

CREATING A TASK SHORTCUT

The application provides the option of creating shortcuts for a quick start of full, quick and vulnerability scan tasks. This can start the required scan without opening the main application window or the context menu.

To create a shortcut to start a scan:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Scan** section, select the **General Settings** subsection.
4. In the right part of the window, in the **Scan tasks quick run** section, click the **Create shortcut** button next to the name of the required task (**Quick Scan**, **Full Scan**, or **Vulnerability Scan**).
5. Specify the path for saving a shortcut and its name in the window that opens. By default, the shortcut is created with the name of a task in the *My Computer* folder of the current computer user.

VULNERABILITY SCAN

Vulnerabilities of the operating system may be caused by errors in programming or design, unreliable passwords, malware activity, and so on. When scanning for vulnerabilities, the application analyzes the system, searches for anomalies and damaged settings of the operating system and web browser, looks for vulnerable services and takes other security-related precautions.

The diagnostics may take some time. When it is complete, found problems are analyzed from the perspective of a possible threat to the system.

After the vulnerability scan task start (see page 46), its progress is displayed in the **Vulnerability Scan** window, in the **Finish** field. Vulnerabilities detected when scanning the system and applications, are displayed in the same window, on the **System vulnerabilities** and **Vulnerable applications** tabs.

When searching for threats, information on the results is logged in a Kaspersky Small Office Security report.

As with virus scan tasks, you can set a start schedule for a vulnerability scan task, create a list of objects to scan (see page 67), specify an account (see section "Running scan under a different user account" on page 68) and create a shortcut for quick start of a task. By default, the applications already installed on the computer are selected as scan objects.

UPDATE

Updating databases and program modules of Kaspersky Small Office Security ensures the up-to-date protection status for your computer. New viruses, Trojans, and other types of malware appear worldwide on a daily basis. Kaspersky Small Office Security databases contain information about threats and ways of eliminating them, so regular application update is required for ensuring your computer's security and for timely detection of new threats.

Regular update requires an active license for application usage. Without a license, you will only be able to update the application once.

Application update downloads and installs the following updates on your computer:

- Kaspersky Small Office Security databases.

  The protection of information is based on databases which contain signatures of threats and network attacks, and the methods used to fight them. Protection components use these databases to search for and disinfect dangerous objects on your computer. The databases are supplemented every hour with records of new threats. Therefore, you are advised to update them on a regular basis.

  In addition to the Kaspersky Small Office Security databases, the network drivers that enable the application's components to intercept network traffic are updated.

- Application modules.

  In addition to the databases of Kaspersky Small Office Security, you can also update the program modules. The update packages fix Kaspersky Small Office Security's vulnerabilities, and supplement or improve the existing functionality.

The main update source of Kaspersky Small Office Security are special Kaspersky Lab update servers. While updating Kaspersky Small Office Security, you can copy database and program module updates received from Kaspersky Lab servers into a local folder, providing access to other networked computers. This saves Internet traffic.

You can also modify automatic update startup settings.

Your computer should be connected to the Internet for successful downloading of updates from our servers. By default, the Internet connection settings are determined automatically. If you use a proxy server, you may need to adjust the connection settings.

During an update, the application modules and databases on your computer are compared with the up-to-date version at the update source. If your current databases and modules differ from those in the actual version of the application, the lacking portion of updates will be installed on your computer.

If the databases are outdated, the update package may be large, which may cause additional Internet traffic (up to several dozen MB).

Prior to updating the databases, Kaspersky Small Office Security creates backup copies of them if you want to roll back to the previous version of databases (see section "Rolling back the last update" on page 76).

Information about the current condition of Kaspersky Small Office Security databases is displayed in the **Update Center** section of the main application window.

Information on the update results and events, which have occurred during the execution of the update task, is logged in a Kaspersky Small Office Security report.

IN THIS SECTION:

Selecting an update source 73

Creating the update startup schedule 75

Rolling back the last update 76

Scanning Quarantine after update 76

Using the proxy server 76

Running updates under a different user account 77

SELECTING AN UPDATE SOURCE

Update source is a resource containing updates for databases and application modules of Kaspersky Small Office Security. You can specify HTTP/FTP servers, local and network folders as update sources.

The main update sources are Kaspersky Lab update servers where database updates and application module updates for all Kaspersky Lab products are stored.

If you do not have access to Kaspersky Lab's update servers (for example, the access to the Internet is restricted), you can call the Kaspersky Lab headquarters (http://www.kaspersky.com/contacts) to request contact information of Kaspersky Lab partners who can provide you with updates on removable media.

When ordering updates on removable media, please specify whether you also require updates for the application modules.

By default, the list of update sources contains only Kaspersky Lab's update servers. If several resources are selected as update sources, Kaspersky Small Office Security tries to connect to them one after another, starting from the top of the list, and retrieves the updates from the first available source.

If you select a resource outside the LAN as an update source, you must have an Internet connection to update.

To choose an update source:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.
4. Click the **Settings** button in the **Update source** section in the right part of the window.
5. In the window that will open, on the **Source** tab, click the **Add** link to open the **Select update source** window.
6. In the **Source** field, select the folder that contains the updates, or enter the address of the server, from which updates should be downloaded.

IN THIS SECTION:

Selecting the update server region..... 74

Updating the application from a shared folder..... 74

SELECTING THE UPDATE SERVER REGION

If you use Kaspersky Lab servers as the update source, you can select the optimal server location when downloading updates. Kaspersky Lab servers are located in several countries.

Using the closest Kaspersky Lab update server allows you to reduce the time period required for receiving updates and increase the operation performance speed. By default, the application uses information about the current region from the operating system's registry. You can select the region manually.

To select the server region:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.
4. Click the **Settings** button in the **Update source** section in the right part of the window.
5. In the window that opens, on the **Source** tab, in the **Regional settings** section, select the **Select from the list** option, and then select the country nearest to your current location from the dropdown list.

UPDATING THE APPLICATION FROM A SHARED FOLDER

To save Internet traffic, you can configure update of Kaspersky Small Office Security from a shared folder when updating the application on networked computers. If done, one of the networked computers receives an update package from Kaspersky Lab servers or from another web resource that contains the required set of updates. The received updates are copied into a shared folder. Other networked computers access this folder to receive updates for Kaspersky Small Office Security.

To enable updates distribution mode:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.
4. In the right part of the window, in the **Additional** section, check the **Copy updates to folder** box and specify the path to a shared folder, where all downloaded updates are copied, in the field below. You can also select a folder by clicking the **Browse** button.

To enable updating the application on a specified computer from the shared folder you have selected:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.
4. Click the **Settings** button in the **Update source** section in the right part of the window.

5. In the window that will open, on the **Source** tab, click the **Add** link to open the **Select update source** window.

6. Select a folder or enter the full path to it in the **Source** field.

7. Uncheck the **Kaspersky Lab update servers** box on the **Source** tab.

CREATING THE UPDATE STARTUP SCHEDULE

You can create a schedule to automatically start an update task: specify task run frequency, start time (if necessary), and advanced settings.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the skipped task to start automatically as soon as it becomes possible.

You can also postpone automatic startup of the task after the application is started. Note that all scheduled tasks will be run only after the specified time interval elapses since the startup of Kaspersky Small Office Security.

- *To configure the update task startup schedule:*

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.

4. Click the **Settings** button in the **Run mode** section in the right part of the window.

5. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select the **By schedule** option and configure the update run mode.

- *To enable automatic launch of skipped task:*

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.

4. Click the **Settings** button in the **Run mode** section in the right part of the window.

5. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and check the **Run skipped tasks** box.

- *To postpone task run after the application startup:*

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.

4. Click the **Settings** button in the **Run mode** section in the right part of the window.

5. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select the **By schedule** option and fill in the **Postpone running after application startup for** field to specify the time to which the task run should be postponed.

ROLLING BACK THE LAST UPDATE

After first update of Kaspersky Small Office Security databases and program modules, the option of rolling back to the previous databases becomes available.

At the start of the update process, Kaspersky Small Office Security creates a backup copy of the current databases and application modules. If necessary, you can restore the previous databases. Update roll back feature is useful in case the new databases version contains an invalid signature that makes Kaspersky Small Office Security block a safe application.

In the event of Kaspersky Small Office Security database damage it is recommended to launch update to download a valid set of databases for up-to-date protection.

To roll back to the previous database version:

1. Open the main application window.

2. Select the **Update Center** section in the left part of the window.

3. Click the **Roll back to the previous databases** button in the right part of the window.

SCANNING QUARANTINE AFTER UPDATE

If the application has scanned an object and has not found out what malicious programs have infected it, the object is quarantined. After the next database update, the product may be able to recognize the threat unambiguously and neutralize it. You can enable the auto scan for quarantined objects after each update.

For this reason, the application scans quarantined objects after each update. Scanning may change their status. Some objects can then be restored to the previous locations, and you will be able to continue working with them.

To enable scanning quarantined files after update:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.

4. In the right part of the window, under **Additional**, check the **Rescan Quarantine after update** box.

USING THE PROXY SERVER

If you use a proxy server for Internet connection, you should reconfigure it to allow proper update of Kaspersky Small Office Security.

To configure the proxy server:

1. Open the main applicationwindow.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.
4. Click the **Settings** button in the **Update source** section in the right part of the window.
5. In the window that opens, on the **Source** tab, click the **Proxy server** button.
6. Configure the proxy server settings in the **Proxy server settings** window that opens.

RUNNING UPDATES UNDER A DIFFERENT USER ACCOUNT

By default, the update procedure is run under your system account. However, Kaspersky Small Office Security can update from a source for which you have no access rights (for example, from a network folder containing updates) or authorized proxy user credentials. You can run Kaspersky Small Office Security updates on behalf of the user account that has such rights.

To start the update under a different user's account:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Update** section, select the **Update Settings** subsection.
4. Click the **Settings** button in the **Run mode** section in the right part of the window.
5. In the window that opens, on the **Run mode** tab, in the **User account** section, check the **Run task as** box. Specify the user name and password.

FILE ANTI-VIRUS

File Anti-Virus prevents infection of the computer's file system. The component starts upon startup of the operating system, continuously remains in the computer's RAM, and scans all files being opened, saved, or launched on your computer and all connected drives.

When the user or a program attempts to access a protected file, File Anti-Virus checks if the iChecker and iSwift databases contain information about this file, and makes a decision on whether the file should be scanned or not.

Kaspersky Lab's specialists advise you not to configure File Anti-Virus settings on your own. In most cases, changing the security level is enough.

If you need to disable the scanning of file system temporarily, you can configure the automatic pausing of File Anti-Virus, or disable File Anti-Virus, if necessary.

You can create a protection scope and choose the object scan mode.

By default, the mode of using records from application databases to search for threats is always enabled. Additionally, you can apply heuristic analysis (see page 81) and various scan technologies (see page 81).

If a threat is detected, Kaspersky Small Office Security assigns one of the following statuses to the found object:

- malicious program (such as a *virus* or *Trojan*);
- *potentially infected* (suspicious) status if the scan cannot determine whether the object is infected or not. The file may contain a sequence of code appropriate for viruses, or modified code from a known virus.

The application displays a notification (see page 222) about the detected threat and performs the assigned action. You can change actions to be performed on detected threat.

If you work in automatic mode (see section "Using interactive protection mode" on page 39), Kaspersky Small Office Security will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**. If you work in interactive mode (see section "Using interactive protection mode" on page 39), Kaspersky Small Office Security displays a notification window, in which you will be able to choose one of the available actions.

Before attempting to disinfect or delete an infected object, Kaspersky Small Office Security creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable the automatic scan for quarantined objects after each update.

IN THIS SECTION:

Enabling and disabling File Anti-Virus 78

Automatically pausing File Anti-Virus 78

Creating a protection scope 79

Changing and restoring security level 80

Changing the scan mode 81

Using heuristic analysis 81

Scan technology 81

Changing actions to be performed on detected objects 82

Scan of compound files 82

Scan optimization 83

ENABLING AND DISABLING FILE ANTI-VIRUS

By default, File Anti-Virus is enabled, functioning in normal mode. You can disable File Anti-Virus, if necessary.

To enable or disable File Anti-Virus, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. In the right part of the window, uncheck the **Enable File Anti-Virus** box if you need to disable this component. Check this box if you need to enable the component.

AUTOMATICALLY PAUSING FILE ANTI-VIRUS

When carrying out resource-intensive works, you can pause File Anti-Virus. To reduce workload and ensure quick access to objects, you can configure automatic pausing of the component at a specified time or when handling specified programs.

Pausing File Anti-Virus when it conflicts with some programs is an emergency operation! If any conflicts arise when working with the component, please contact Kaspersky Lab Technical Support Service (http://support.kaspersky.com). The support specialists will help you resolve the simultaneous operation of Kaspersky Small Office Security with other applications on your computer.

To pause the component at a specified time:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Additional** tab, in the **Pause task** section, check the **By schedule** box and click the **Schedule** button.
6. In the **Pause task** window, specify the time (in 24-hour hh:mm format) for which protection will be paused (**Pause task at** and **Resume task at** fields).

To pause the component when running specified applications:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that will open, on the **Additional** tab, in the **Pause task** section, check the **At application startup** box and click the **Select** button.
6. In the **Applications** window create a list of applications which pause the component when running.

CREATING A PROTECTION SCOPE

Protection scope is the location of objects being scanned and the types of files to be scanned. By default, Kaspersky Small Office Security scans only potentially infectable files stored on any hard drive, network drive or removable media.

You can expand or restrict the protection scope by adding / removing objects to be scanned or changing the type of files to be scanned. For example, you can only select EXE files run from network drives to be scanned.

When selecting file types please remember the following:

- Probability of malicious code penetrating several file formats (such as .txt) and its further activation is quite low. At the same time, there are formats that contain or may contain an executable code (such as .exe, .dll, .doc). The risk of penetrating and activating malicious code in such files is quite high.
- The intruder can send a virus to your computer in an executable file renamed as txt file. If you have selected the scan of files by extension, such a file is skipped by the scan. If the scan of files by format is selected, then, regardless of the extension, File Anti-Virus will analyze the file header, and reveal that the file is an .exe file. Such a file would be thoroughly scanned for viruses.

To edit the object scan list:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **General** tab, in the **Protection scope** section, open the object selection window by clicking the **Add** link.
6. In the **Select object to scan** window, select an object and click the **Add** button.
7. After you have added all required objects, click the **OK** button in the **Select object to scan** window.
8. To remove an object from the scan list, uncheck the box next to it.

To change the type of scanned objects:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **General** tab, in the **File types** section, select the required settings.

CHANGING AND RESTORING SECURITY LEVEL

Depending on your actual needs, you can select one of the preset file/memory security levels or configure File Anti-Virus on your own.

When configuring File Anti-Virus, you can always roll back to the recommended values. These values are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

Before enabling the low security level, it is recommended to perform the full scan of computer (see section "How to perform full scan of your computer for viruses" on page 46) at high security level.

To change the current file and memory security level:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. In the right part of the window, in the **Security level** section, set the required security level, or click the **Settings** button to modify the settings manually.

   If you modify the settings manually, the name of the security level will change to **Custom**.

To restore the default protection settings:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. Click the **Default level** button in the **Security level** section in the right part of the window.

CHANGING THE SCAN MODE

The scan mode is the condition which triggers File Anti-Virus into activity. The default setting for Kaspersky Small Office Security is smart mode, which determines if the object is subject to scanning on the basis of the actions performed in respect of it. For example, when working with a Microsoft Office document, Kaspersky Small Office Security scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

You can change the object scan mode. The scan mode should be selected depending on the files you work with most of the time.

To change the object scan mode:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens on the **Additional** tab, in the **Scan mode** section, select the required mode.

USING HEURISTIC ANALYSIS

During File Anti-Virus operation, *signature analysis* is always used: Kaspersky Small Office Security compares the object found with the database records.

To improve protection efficiency, you can use the *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis allows detecting new malicious objects which are not yet described in the databases.

To enable or disable the heuristic analysis:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Performance** tab, in the **Scan methods** section, check the **Heuristic analysis** box and specify the detail level for the scan. Uncheck the **Heuristic Analysis** box if that scanning method should not be used.

SCAN TECHNOLOGY

In addition to the heuristic analysis you can use special technologies, allowing an increase in the objects scan speed by excluding the files that have not been modified since they were last scanned.

To enable the object scan technologies:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Additional** tab, in the **Scan technologies** section, select the required values.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If infected or potentially infected objects are detected, the application performs an action depending on the selected operation mode: automatic or interactive (see section "File Anti-Virus" on page 77). You can modify the specified action.

To change the specified action to be performed on detected objects:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

4. In the left part of the window, in the **Action** section, select the required action.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden in this way a compound file should be unpacked, which can significantly lower the scan speed.

For each type of compound file, you can select to scan either all files or only new ones.

By default, Kaspersky Small Office Security scans only embedded OLE objects. Installer packages and files containing OLE objects are executed when they are opened, which makes them more dangerous than archives.

When large compound files are scanned, their preliminary unpacking may take a long period of time. This period can be reduced by enabling unpacking of compound files in background mode if they exceed the specified file size. If a malicious object is detected while working with such a file, the application will notify you about it.

You can restrict the maximum size of the compound file being scanned. Compound files larger than the specified value will not be scanned.

To modify the list of scanned compound files:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Performance** tab, in the **Scan of compound files** section, select the required type of compound files to be scanned.

In order to set the maximum size of compound files to be scanned:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.

6. In the **Compound files** window, check the **Do not unpack large compound files** box and specify the maximum file size.

When large files are extracted from archives, they will be scanned even if the **Do not unpack large compound files** box is checked.

To unpack large-sized compound files in background mode:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.

6. In the **Compound files** window, check the **Extract compound files in the background** box and specify the minimum file size.

SCAN OPTIMIZATION

You can shorten the scan time and speed up Kaspersky Small Office Security. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

To scan only new and changed files:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Performance** tab, in the **Scan optimization** section, check the **Scan only new and changed files** box.

MAIL ANTI-VIRUS

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Mail Anti-Virus scans incoming and outgoing messages for malicious objects. It starts when the operating system boots and runs continually, scanning all email messages sent or received via the POP3, SMTP, IMAP, MAPI, and NNTP protocols, as well as over encrypted connections (SSL) via POP3 and IMAP (see section "Scanning encrypted connections" on page 133).

The indicator of the component's operation is the application icon in the taskbar notification area, which looks like whenever an email message is being scanned.

The application intercepts each message that the user sends or receives and parses it into basic components: message header, body, attachments. Message body and attachments (including attached OLE objects) are scanned for the presence of threats.

Kaspersky Lab advises you not to configure Mail Anti-Virus settings on your own. In most cases, selecting a security level is enough (see section "Changing and restoring security level" on page 86).

You can specify the types of messages to be scanned, and specify which scan methods should be used. By default, the mode of using records from application databases to search for threats is always enabled. In addition, you can enable heuristic analysis. Furthermore, you can enable filtering of attachments (see page 87), which allows automatic renaming or deletion of specified file types.

If a threat is detected, Kaspersky Small Office Security assigns one of the following statuses to the found object:

- malicious program (such as a *virus* or *Trojan*);
- *potentially infected* (suspicious) status if the scan cannot determine whether the object is infected or not. The file may contain a sequence of code appropriate for viruses, or modified code from a known virus.

The application blocks a message, displays a notification (see page 222) about the detected threat and performs the assigned action. You can change actions to be performed on detected threat (see section "Changing actions to be performed on detected objects" on page 87).

If you work in automatic mode (see section "Using interactive protection mode" on page 39), Kaspersky Small Office Security will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**. If you work in interactive mode (see section "Using interactive protection mode" on page 39), Kaspersky Small Office Security displays a notification window, in which you will be able to choose one of the available actions.

Before attempting to disinfect or delete an infected object, Kaspersky Small Office Security creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable the automatic scan for quarantined objects after each update.

After the email message is successfully disinfected, it returns to the user. If the disinfection fails, the infected object is deleted from the message. After the virus scan, a special text is inserted in the subject line of the email, stating that the email was processed by Kaspersky Small Office Security.

You can disable Mail Anti-Virus, if necessary (see section "Enabling and disabling Mail Anti-Virus" on page 85).

An integrated plug-in is provided for Microsoft Office Outlook (see section "Email scanning in Microsoft Office Outlook" on page 88) that allows you to fine-tune the email client.

If you use The Bat!, Kaspersky Small Office Security can be used in conjunction with other anti-virus applications. At that, the email traffic processing rules (see section "Email scanning in The Bat!" on page 88) are configured directly in The Bat! and override the application's email protection settings.

When working with other mail programs, including Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora, and Incredimail, the Mail Anti-Virus component scans email on SMTP, POP3, IMAP, and NNTP protocols.

Note that when working with the Thunderbird mail client, email messages transferred via IMAP will not be scanned for viruses if any filters moving messages from the **Inbox** folder are used.

IN THIS SECTION:

Enabling and disabling Mail Anti-Virus 85

Creating a protection scope 85

Changing and restoring security level 86

Using heuristic analysis 86

Changing actions to be performed on detected objects 87

Attachment filtering 87

Scan of compound files 87

Email scanning in Microsoft Office Outlook 88

Email scanning in The Bat! 88

ENABLING AND DISABLING MAIL ANTI-VIRUS

By default, Mail Anti-Virus is enabled, functioning in normal mode. You can disable Mail Anti-Virus, if necessary.

To enable or disable Mail Anti-Virus, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
4. In the right part of the window, uncheck the **Enable Mail Anti-Virus** box if you need to disable this component. Check this box if you need to enable the component.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages to be scanned. By default, Kaspersky Small Office Security scans both incoming and outgoing emails.

If you have selected scan only incoming messages, you are advised to scan outgoing email when you first begin using Kaspersky Small Office Security since it is likely that there are worms on your computer which will distribute themselves via email. This will avoid unpleasant situations caused by unmonitored mass emailing of infected emails from your computer.

The protection scope also includes the settings used to integrate the Mail Anti-Virus component into the system, and the protocols to be scanned. By default, the Mail Anti-Virus component is integrated into the Microsoft Office Outlook and The Bat! email client applications.

To disable scans of outgoing emails:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. Use the **General** tab of the displayed window to select in the **Protection scope** section the option **Incoming messages only**.

To select the protocols to scan and the settings to integrate Mail Anti-Virus into the system:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Additional** tab, in the **Connectivity** section select the required settings.

CHANGING AND RESTORING SECURITY LEVEL

Depending on your actual needs, you can select one of the preset email security levels or configure Mail Anti-Virus on your own.

When configuring File Anti-Virus, you can always roll back to the recommended values. These values are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To change the preset email security level:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.

4. In the right part of the window, in the **Security level** section, set the required security level, or click the **Settings** button to modify the settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

To restore default mail protection settings:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.

4. Click the **Default level** button in the **Security level** section in the right part of the window.

USING HEURISTIC ANALYSIS

During Mail Anti-Virus operation, *signature analysis* is always used: Kaspersky Small Office Security compares the object found with the database records.

To improve protection efficiency, you can use the *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis allows detecting new malicious objects which are not yet described in the databases.

To enable or disable the heuristic analysis:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **General** tab, in the **Scan methods** section, check the **Heuristic analysis** box and specify the detail level for the scan. Uncheck the **Heuristic Analysis** box if that scanning method should not be used.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If infected or potentially infected objects are detected, the application performs an action depending on the selected operation mode: automatic or interactive. You can modify the specified action.

To change the specified action to be performed on detected objects:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
4. In the left part of the window, in the **Action** section, select the required action.

ATTACHMENT FILTERING

Malware is most often distributed in mail as objects attached to messages. To protect your computer, for example, from automatic launch of attached files, you can enable filtering of attachments, which can automatically rename or delete files of specified types.

To enable filtering of attachments:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. Use the **Attachment filter** tab of the displayed window to select the filtering mode for attachments. When you select either of the last two modes, the list of file types (extensions) will become enabled; there you can select the required types or add a mask to select a new type.

   To add a new type mask to the list, click the **Add** link to open the **Input file name mask** window and enter the necessary data.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden in this way a compound file should be unpacked, which can significantly lower the scan speed.

You can enable or disable the scan of attached archives and limit the maximum size of archives to be scanned.

If your computer is not protected by any local network software (you access the Internet directly without a proxy server or a firewall), it is not recommended to disable the scanning of attached archives.

To configure the settings for the scan of compound files:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. Use the **General** tab in the displayed window to define necessary settings.

EMAIL SCANNING IN MICROSOFT OFFICE OUTLOOK

If you are using Microsoft Office Outlook as your mail client, you may modify additional settings for scanning your mail for viruses.

When installing Kaspersky Small Office Security, a special plug-in is installed in Microsoft Office Outlook. It allows you to configure Mail Anti-Virus settings quickly, and determine when email messages are scanned for dangerous objects.

The plug-in comes in the form of **Email protection** tab located in the **Tools** → **Options** menu.

To define the proper time for mail scanning, perform the following steps:

1. Open the main Microsoft Outlook application window.
2. Select **Tools** → **Options** from the application menu.
3. Use the **Email protection** tab to select necessary settings.

EMAIL SCANNING IN THE BAT!

Actions in respect of infected email objects in The Bat! are defined using the application's own tools.

Mail Anti-Virus settings determining if incoming and outgoing messages should be scanned, which actions should be performed in respect of dangerous objects in email, and which exclusions should apply, are ignored. The only thing that The Bat! takes into account is the scanning of attached archives.

The email protection settings extend to all the anti-virus components installed on the computer that support working with the Bat!.

Note that incoming email messages are first scanned by Mail Anti-Virus and only after that – by the plug-in of The Bat!. If a malicious object is detected, Kaspersky Small Office Security immediately notifies you of this event. If you select the **Disinfect** (**Delete**) action in the notification window of Mail Anti-Virus, actions aimed at eliminating the threat are performed by Mail Anti-Virus. If you select the **Ignore** option in the notification window, the object will be disinfected by the plug-in of The Bat!. When sending email messages, they are first scanned by the plug-in and then - by Mail Anti-Virus.

You have to define the following criteria:

- which mail stream (incoming, outgoing) should be scanned;
- when the mail objects should be scanned (when opening a message, before saving to disk);

- what actions are performed by the mail client if dangerous objects are detected in email messages. For example, you could select:
  - **Attempt to disinfect infected parts** – if this option is selected, the attempt is made to disinfect the infected object; if it cannot be disinfected, the object remains in the message.
  - **Delete infected parts** – if this option is selected, the dangerous object in the message is deleted regardless of whether it is infected or suspected to be infected.

By default, The Bat! places all infected email objects in Quarantine without attempting to disinfect them.

The Bat! does not give special headers to emails containing dangerous objects.

To set up email protection rules in The Bat!:

1. Open the main The Bat! window.
2. Select the **Settings** item from the **Properties** menu of the mail client.
3. Select the **Virus protection** object from the settings tree.

WEB ANTI-VIRUS

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Whenever you use the Internet, the information stored on your computer becomes subject to the risk of infection from dangerous programs. These can infiltrate your computer while you are downloading free software, or browsing known safe websites, which have been subject to hacker attacks before you have gone on them. Moreover, network worms can penetrate your computer before you open a webpage or download a file just because your computer is connected to the Internet.

The *Web Anti-Virus* component is designed to ensure security while using the Internet. It protects your computer against data coming in via the HTTP, HTTPS and FTP protocols, and also prevents dangerous scripts from being executed on the computer.

Web protection monitors the data stream that passes only through the ports included in the monitored port list. A list of ports that are most commonly used for data transfer is included in the Kaspersky Small Office Security installation package. If you use any ports that are not included in this list, add them into the list of monitored ports (see section "Creating a list of monitored ports" on page 135) to ensure protection of data streams being directed via them.

A collection of settings called the security level, determines how data stream will be scanned (see section "Changing and restoring security level" on page 91). If Web Anti-Virus detects a threat, it will perform the assigned action.

Kaspersky Lab advises you not to configure Web Anti-Virus settings on your own. In most cases, it is enough to select an appropriate security level.

Component operation algorithm

Web Anti-Virus protects the data reaching your computer and transferred from it over HTTP, HTTPS and FTP, and prevents hazardous scripts from running on the computer. By default, scan of secure connections (via HTTPS) is disabled, you can enable and configure it (see section "Scanning encrypted connections" on page 133).

Data is protected using the following algorithm:

1. Each web page or file that is accessed by the user or an application via the HTTP, HTTPS or FTP protocols, is intercepted and analyzed for malicious code by Web Anti-Virus. Malicious objects are detected using both Kaspersky Small Office Security databases and the heuristic algorithm. The database contains descriptions of all the malicious programs known to date and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the database.

2. After the analysis, you have the following courses of action available:

   - If a web page or an object accessed by the user contains malicious code, access to them is blocked. A notification is displayed that the object or page being requested is infected.

   - If the file or web page does not contain malicious code, the program immediately grants the user access to it.

Scripts are scanned according to the following algorithm:

1. Each script run is intercepted by Web Anti-Virus and is analyzed for malicious code.

2. If the script contains malicious code, Web Anti-Virus blocks this script and informs the user of it with a special pop-up message.

3. If no malicious code is discovered in the script, it is run.

Web Anti-Virus intercepts only scripts using the Microsoft Windows Script Host functionality.

IN THIS SECTION:

Enabling and disabling Web Anti-Virus 90

Changing and restoring security level 91

Changing actions to be performed on detected objects 91

Blocking dangerous scripts 92

Checking URLs using the databases of suspicious and phishing addresses 92

Using heuristic analysis 92

Scan optimization 93

Kaspersky URL Advisor 93

Creating a list of trusted addresses 94

ENABLING AND DISABLING WEB ANTI-VIRUS

By default, Web Anti-Virus is enabled, functioning in normal mode. You can disable Web Anti-Virus, if necessary.

To enable or disable Web Anti-Virus, perform the following steps:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.

4. In the right part of the window, uncheck the **Enable Web Anti-Virus** box if you need to disable this component. Check this box if you need to enable the component.

CHANGING AND RESTORING SECURITY LEVEL

Depending on your actual needs, you can select one of the preset security levels or configure Web Anti-Virus on your own.

When configuring File Anti-Virus, you can always roll back to the recommended values. These values are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To change the preset security level for web traffic:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.

4. In the right part of the window, in the **Security level** section, set the required security level, or click the **Settings** button to modify the settings manually.

   If you modify the settings manually, the name of the security level will change to **Custom**.

To restore default Web traffic protection settings:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.

4. Click the **Default level** button in the **Security level** section in the right part of the window.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If infected or potentially infected objects are detected, the application performs an action depending on the selected operation mode: automatic or interactive.

If you work in automatic mode (see section "Using interactive protection mode" on page 39), Kaspersky Small Office Security will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**. If you work in interactive mode (see section "Using interactive protection mode" on page 39), Kaspersky Small Office Security displays a notification window, in which you will be able to choose one of the available actions.

To change the specified action to be performed on detected objects:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.

4. In the right part of the window, in the **Action** section, select the required action.

BLOCKING DANGEROUS SCRIPTS

Web Anti-Virus can scan all scripts processed in Microsoft Internet Explorer, as well as any other WSH scripts (JavaScript, Visual Basic Script, etc.) launched when the user works on the computer. If a script presents a threat to your computer, it will be blocked.

In order for Web Anti-Virus to scan and block scripts:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the **Web Anti-Virus** window that opens, in the **Additional** block, the **Block dangerous scripts in Microsoft Internet Explorer** box should be checked. If this box is unchecked, enable it.

CHECKING URLS USING THE DATABASES OF SUSPICIOUS AND PHISHING ADDRESSES

Web Anti-Virus scans web traffic for viruses and checks the links if they are included in the list of suspicious or phishing web addresses.

Checking the links if they are included in the list of phishing addresses allows avoiding phishing attacks, which look like email messages from would-be financial institutions and contain links to the websites of these organizations. The message text convinces the reader to click the link and enter confidential information in the window that opens, for example, a credit card number or a login and password for an Internet banking web page where financial operations can be carried out. A phishing attack can be disguised, for example, as a letter from your bank with a link to its official website. By clicking the link, you go to an exact copy of the bank's website and can even see the real address in the browser, even though you are actually on a counterfeit site. From this point forward, all your actions on the site are tracked and can be used to steal your money.

The lists of phishing URLs are included with the Kaspersky Small Office Security delivery set. Since links to phishing web sites may be received not only in email, but also from other sources, such as ICQ messages, Web Anti-Virus monitors attempts to access a phishing web site on the level of web traffic and blocks access to such locations.

To configure Web Anti-Virus to check URLs against the databases of suspicious and phishing web addresses, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the **Web Anti-Virus** window that will open, in the **Scan methods** section, the **Check if URLs are listed in the base of suspicious web addresses** box and the **Check if URLs are listed in the base of phishing web addresses box** should be checked. If these boxes are unchecked, enable them.

USING HEURISTIC ANALYSIS

During Mail Anti-Virus operation, *signature analysis* is always used: Kaspersky Small Office Security compares the object found with the database records.

To improve protection efficiency, you can use the *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis allows detecting new malicious objects which are not yet described in the databases.

To enable or disable the heuristic analysis:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the **Web Anti-Virus window** that opens, in the **Scan methods** section, check the **Heuristic analysis** box and specify the detail level for the scan. Uncheck the **Heuristic Analysis** box if that scanning method should not be used.

SCAN OPTIMIZATION

To detect malicious code more efficiently, Web Anti-Virus caches fragments of objects downloaded from the Internet. However, buffering objects increases object processing time. This can cause problems when copying and processing large objects. To optimize work with objects downloaded from the Internet, you can limit the buffering time of objects' fragments.

To limit traffic caching time:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the **Web Anti-Virus** window that opens, in the **Scan optimization** section, check the **Limit traffic caching time** box and enter the time value (in seconds) in the field to the right.

KASPERSKY URL ADVISOR

Kaspersky Small Office Security includes the URL scanning module managed by Web Anti-Virus. This module is built into Microsoft Internet Explorer and Mozilla Firefox browsers as a plug-in.

This module checks if links located on the webpage belong to the list of suspicious and phishing web addresses. You can create a list of web addresses whose content will not be checked for the presence of suspicious or phishing URLs, or a list of web sites whose content must be scanned. You can also completely exclude scan of URLs.

To enable the URL scanning module, please do the following:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the **Web Anti-Virus** window that will open, in the **Additional** section, check the **Mark phishing and suspicious URLs in Microsoft Internet Explorer and Mozilla Firefox** box.

To create a list of websites whose content will not be scanned for the presence of suspicious or phishing URLs:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the **Web Anti-Virus** window that opens, in the **Additional** section, click the **Settings** button.
6. In the **Kaspersky URL advisor** window that will open, select the **On all web pages** option and click the **Exclusions** button.
7. In the **List of trusted web addresses** window that opens, create the list of web addresses, the content of which should not be scanned for suspicious or phishing URLs.

To create a list of websites whose content should be scanned for suspicious or phishing URLs:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the **Web Anti-Virus** window that opens, in the **Additional** section, click the **Settings** button.
6. In the **Kaspersky URL advisor** window that will open, select the **On the selected web pages** option and click the **Select** button.
7. In the **List of checked web addresses** window that opens, create the list of web addresses, the content of which must be scanned for suspicious or phishing URLs.

CREATING A LIST OF TRUSTED ADDRESSES

You can create a list of web addresses whose content you unconditionally trust. Web Anti-Virus will not analyze data from those addresses for dangerous objects. This option may be useful, for instance, when Web Anti-Virus interferes with downloading a particular file from a known website.

To create the list of trusted web addresses:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the **Web Anti-Virus** window that will open, in the **Scan optimization** section, check the **Do not scan HTTP traffic from trusted web addresses** box and click the **Select** button.
6. In the **List of trusted web addresses** window that opens, create the list of addresses providing trusted content.

If you need to exclude an address from the trusted list temporarily, you do not have to delete it – unchecking its box to the left will produce the necessary effect.

IM ANTI-VIRUS

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

IM Anti-Virus scans the traffic of instant messaging clients (the so-called *Internet pagers*).

IM messages may contain links to suspicious web sites and to the web sites deliberately used by hackers to organize phishing attacks. Malicious programs use IM clients to send spam messages and links to the programs (or the programs themselves), which steal users' ID numbers and passwords.

Kaspersky Small Office Security ensures safe operation of various instant messaging applications, including ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent and IRC.

Some IM clients, such as Yahoo! Messenger and Google Talk, use encrypted connections. To scan the traffic generated by those programs, you have to enable scanning for secure connections (see page 133).

IM Anti-Virus intercepts the messages checking them for the presence of dangerous objects or URLs. You can select the types of messages (see page 95) to scan and various scanning methods.

If threats are detected in a message, IM Anti-Virus substitutes this message with a warning message for the user.

Files transferred via IM clients are scanned by the File Anti-Virus (on page 77) component when they are attempted to save.

IN THIS SECTION:

Enabling and disabling IM Anti-Virus 95

Creating a protection scope 95

Selecting the scan method 96

ENABLING AND DISABLING IM ANTI-VIRUS

By default, IM Anti-Virus is enabled, functioning in normal mode. You can disable IM Anti-Virus, if necessary.

To enable or disable IM Anti-Virus, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
4. In the right part of the window, uncheck the **Enable IM Anti-Virus** box if you need to disable this component. Check this box if you need to enable the component.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages to be scanned. By default, Kaspersky Small Office Security scans both incoming and outgoing emails. If you are sure that messages sent by you cannot contain any dangerous objects, you may disable the scan of outgoing traffic.

To disable the scan of outgoing messages:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
4. In the right part of the window, in the **Protection scope** section, select the **Incoming messages only** option.

SELECTING THE SCAN METHOD

Scan methods consist in scanning URLs in IM clients' messages to know if they are included in the list of suspicious URLs and / or in the list of phishing URLs.

To improve protection efficiency, you can use the *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis allows detecting new malicious objects which are not yet described in the databases. When using heuristic analysis, any script included in an IM client's message is executed in a protected environment. If this script's activity is typical of malicious objects, the object is likely to be classed as malicious or suspicious. By default, heuristic analysis is enabled.

To scan links in the messages using the database of suspicious web addresses:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
4. In the right part of the window, in the **Scan methods** section, check the **Check if URLs are listed in the database of suspicious URLs** box.

To scan links in the messages using the database of phishing web addresses:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
4. In the right part of the window, in the **Scan methods** section, check the **Check if URLs are listed in the database of phishing URLs** box.

To enable the heuristic analysis:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
4. In the right part of the window, in the **Scan methods** section, check the **Heuristic analysis** box and define the necessary scanning intensity level.

ANTI-SPAM

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Kaspersky Small Office Security includes *Anti-Spam*, a component that allows detection of unwanted messages (spam) and their processing in accordance with the rules in your e-mail client. It saves time while working with e-mail.

Anti-Spam is built into the following mail clients as a plug-in:

- Microsoft Office Outlook (on page 111);
- Microsoft Outlook Express (Windows Mail) (on page 111);
- The Bat! (on page 112);
- Thunderbird (on page 113).

You can use the lists of blocked and allowed senders to specify for Anti-Spam the addresses from which messages will be recognized as useful mail or spam. You may also assign the status of spam to the messages which are not addressed to you directly (see page 106). Furthermore, Anti-Spam can check a message for the presence of allowed and blocked phrases and also for phrases from the list of obscene expressions.

To enable efficient recognition of spam and useful mail by Anti-Spam, the component needs training (see section "Training Anti-Spam" on page 99).

Component operation algorithm

Anti-Spam uses a self-training algorithm that allows the component to tell spam from useful mail better with time. The source of data for the algorithm is the contents of the message.

Anti-Spam work consists of two stages:

1. Application of strict filtering criteria to a message. These criteria allow a quick determination as to whether the message is spam. Anti-Spam assigns to the message *spam* or *not spam* status, the scan is stopped and the message transferred to the mail client for processing (see algorithm steps 1 to 5 below).
2. Inspection of messages, which have passed strict selection criteria during previous steps. Such messages cannot be unambiguously considered spam. Therefore, Anti-Spam has to calculate for them the *probability* of being spam.

The Anti-Spam algorithm consists of the following steps:

1. The message sender's address is checked for its presence in the lists of allowed or blocked senders.
   - If a sender's address is in the allowed list, the message receives the *Not Spam* status.
   - If a sender's address is in the black list, the message receives the *Spam* status.
2. If a message was sent using Microsoft Exchange Server and scan of such messages is disabled, the message is considered as *not spam*.
3. A message analysis is performed to check if it contains strings from the list of allowed phrases. If at least one line from this list has been found, the message will be assigned the *not spam* status. This step is skipped by default.

4. Anti-Spam analyzes a message to check if it contains strings from the list of blocked phrases or the list of obscene words. Whenever words from these lists are found in a message, their weighting coefficients are summed up. If the total of coefficients exceeds 100, such message will receive the *spam* status. This step is skipped by default.

5. If the message text contains an address included in the database of phishing or suspicious web addresses, the message receives the *Spam* status.

6. E-mail is analyzed using heuristic rules. If the analysis finds in a message signs typical of spam, the probability of it being spam increases.

7. E-mail is analyzed using the GSG technology. While doing it, Anti-Spam analyzes images attached to the email message. If the analysis finds in them signs typical of spam, the probability of the message being spam increases.

8. The application analyzes e-mail attachments in .rtf format. It scans attached documents checking them for the presence of spam signs. Once the analysis is complete, Anti-Spam calculates how much the probability of the message being spam increased. The technology is disabled by default.

9. It checks for the presence of the additional features typical of spam. Each detected feature increases the probability that the message being scanned is in fact spam.

10. If Anti-Spam was trained, the message will be scanned using iBayes technology. The self-training iBayes algorithm calculates the probability of a message being spam based on the frequency of phrases typical of spam found in message text.

Message analysis determines the probability of its being spam expressed as the *spam rate* value. The *Spam* or *Probable spam* status will be assigned to a message depending upon the specified threshold values of the spam rate (see section "Regulating threshold values of spam rate" on page 108). The product adds by default to the **Subject** field of spam and potential spam messages the label **[!! SPAM]** or **[?? Probable Spam]** (see section "**Adding a label to the message subject**" on page 109). Then each message will be processed in accordance with your rules defined for e-mail clients (see section "Configuring spam processing by mail clients" on page 111).

IN THIS SECTION:

Enabling and disabling Anti-Spam 99

Changing and restoring security level 99

Training Anti-Spam 99

Scanning links in messages 102

Detecting spam by phrases and addresses. Creating lists 103

Regulating threshold values of spam rate 108

Using additional spam filtering features 108

Selecting the spam recognition algorithm 109

Adding a label to the message subject 109

Filtering email messages at the server. Mail Dispatcher 110

Excluding Microsoft Exchange Server messages from the scan 110

Configuring spam processing by mail clients 111

ENABLING AND DISABLING ANTI-SPAM

By default, Anti-Spam is enabled, functioning in normal mode. You can disable Anti-Spam, if necessary.

To enable or disable Anti-Spam, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. In the right part of the window, uncheck the **Enable Anti-Spam** box if you need to disable this component. Check this box if you need to enable the component.

CHANGING AND RESTORING SECURITY LEVEL

Depending on your actual needs, you can select one of the preset security levels or configure Anti-Spam on your own.

When configuring File Anti-Virus, you can always roll back to the recommended values. These values are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

In order to change the selected Anti-Spam component security level:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. In the right part of the window, in the **Security level** section, set the required security level, or click the **Settings** button to modify the settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

To restore default Anti-Spam settings:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Default level** button in the **Security level** section in the right part of the window.

TRAINING ANTI-SPAM

One of the most powerful spam detection tools is the self-training iBayes algorithm. The application uses the algorithm to decide, which status should be assigned to a message based on the phrases it contains. Prior to work beginning, sample strings of useful and spam mail should be submitted to the iBayes algorithm, i.e. it should be *trained*.

There are several approaches to training Anti-Spam:

- Use the Training Wizard (packet training). Training with the Training Wizard is preferable from the very onset of using Anti-Spam.
- Training Anti-Spam using outgoing messages.

- Training is performed right while working with messages in mail client using the appropriate buttons and menu items.
- Training when working with Anti-Spam reports.

IN THIS SECTION:

Using the Training Wizard 100

Training with outgoing mail 100

Using mail client interface elements 101

Adding an address to the list of allowed senders 101

Training with reports 102

USING THE TRAINING WIZARD

The Training Wizard allows Anti-Spam training in batch mode. To do so, specify which folders of Microsoft Office Outlook or Microsoft Outlook Express (Windows Mail) accounts contain spam and which contain useful mail.

Correct spam recognition requires training using at least 50 samples of useful messages and 50 samples of unwanted mail. iBayes will not be operational until these steps are completed.

To save time, the Training Wizard only trains on 50 emails in each the selected folder.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the Wizard:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Train** button in the **Anti-Spam training** section within the right part of the window.

While training using good mail, the application will automatically add addresses of the corresponding message senders to the list of allowed senders. You can disable the feature (see section "Adding an address to the list of allowed senders" on page 101).

TRAINING WITH OUTGOING MAIL

You can train Anti-Spam using a sample of 50 outgoing emails. Once training is enabled, Anti-Spam will analyze every message you send using it as a sample of useful mail. Training will complete after you send the 50th message.

To enable Anti-Spam training on outgoing emails:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Additional** tab, in the **Outgoing messages** block, check the **Train using outgoing email messages** box.

While training using outgoing mail is in progress, the addresses of mail recipients are automatically added to the list of allowed senders. You can disable the feature (see section "Adding an address to the list of allowed senders" on page 101).

USING MAIL CLIENT INTERFACE ELEMENTS

Training Anti-Spam while working directly with email messages involves using special interface elements of your mail client program.

Buttons used for training Anti-Spam appear in the interface of Microsoft Office Outlook and Microsoft Outlook Express (Windows Mail) mail clients only after you have installed Kaspersky Small Office Security.

To train Anti-Spam using the email client:

1. Start the email client.

2. Select a message with which you wish to train Anti-Spam.

3. Perform the following steps depending upon your email client:

   - click the **Spam** or **Not Spam** button in the Microsoft Office Outlook toolbar;
   - click the **Spam** or **Not Spam** button in the Microsoft Outlook Express toolbar (Windows Mail);
   - use the special **Mark as Spam** and **Mark as Not Spam** items in the **Special** menu of The Bat! email client;
   - use the **Spam / Not Spam** button in the Mozilla Thunderbird toolbar.

After selecting an action from the list above, Anti-Spam performs training using the selected message. If you select several messages, all of them are used for training.

If a message is marked as useful mail, the address of its sender will be added to the list of allowed senders.

ADDING AN ADDRESS TO THE LIST OF ALLOWED SENDERS

When Anti-Spam is trained using regular mail in Training Wizard or directly in the mail client, the addresses of useful mail senders are automatically added to the list of allowed senders (see section "Blocked and allowed senders" on page 105). The application also adds to that list the addresses of outgoing mail recipients if the component training with outgoing mail is used.

You can disable that functionality to prevent automatic addition of allowed senders to the list in the course of training.

To disable adding the address to the list of allowed senders:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Exact methods** tab, in the **Consider message as not spam** block, check the **If it is from an allowed sender** box and click the **Select** button.

   The **Allowed senders** window opens.

6. Uncheck the **Add allowed senders' addresses when training Anti-Spam** box.

TRAINING WITH REPORTS

There is an opportunity to train Anti-Spam using its reports with the information about messages recognized as probable spam. Essentially, the training means assigning the **Spam** or **Not Spam** labels to messages and also their addition to the lists of allowed or blocked senders.

To train Anti-Spam using a report:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Small Office Security.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
4. The **Detailed report** window opens.
5. In the top left part of the window, select the **Anti-Spam** component in the dropdown list.
6. Use the records in the **Object** column in the right part of the window to identify the messages, which you wish to use for Anti-Spam training. For each such message, open the shortcut (right-click) menu and select one of the menu commands corresponding to the operation, which should be performed with the message:
   - Mark as Spam.
   - Mark as Not Spam.
   - Add to the allowed list.
   - Add to the blocked list.

SCANNING LINKS IN MESSAGES

Anti-Spam can check the URLs in mail messages to identify the ones included in the lists of suspicious web addresses or phishing web addresses. These lists are included into the product package of Kaspersky Small Office Security. If a phishing or suspicious link is detected in a message, or if phishing elements are detected in the message body, this message is recognized as spam.

To enable URL checks using the databases of suspicious and phishing addresses:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Exact methods** tab, in the **Consider message as spam** section, check the **If it contains URLs from the database of suspicious URLs** and **If it contains phishing elements** boxes.

DETECTING SPAM BY PHRASES AND ADDRESSES. CREATING LISTS

You can create lists of allowed, blocked and obscene key phrases as well as lists of allowed and blocked sender addresses and the list of your addresses. If these lists are used, Anti-Spam analyzes every message to check if it contains the phrases added to the lists and the addresses of mail sender and recipients to check if they match the records in address lists. Once the sought phrase or address is found, Anti-Spam identifies such message as useful mail or spam depending upon the list where the phrase or address is present.

The following mail will be recognized as spam:

- messages containing blocked or obscene phrases with total weighting coefficient exceeding 100;
- messages sent from a blocked address or not addressed to you directly.

The following messages will be recognized as useful mail:

- messages containing allowed phrases;
- messages sent from an allowed address.

Masks for key phrases and sender addresses

You can use *phrase masks* in the lists of allowed, blocked and obscene phrases. The lists of allowed and blocked addresses, and the list of trusted addresses support *address masks*.

Mask is a template string that a phrase or an address is compared against. Certain symbols in a mask are used to represent others: ***** substitutes any sequence of characters, **?** – any single character. If a mask uses such wildcards, it can match several phrases or addresses (see examples).

If the ***** or **?** character is a part of the sought phrase (e.g., *What's the time?*), it should be preceded with the **** character to ensure that Anti-Spam recognizes it correctly. Thus, instead of the ***** character you should use in masks the ***** combination, the **?** character should be represented as **\?** (e.g., *What's the time**?*).

Sample phrase masks:

- *Visit our ** – this mask corresponds to a message that begins with the words *Visit our* and continues with any text.

Examples of address masks:

- *admin@test.com* – the mask only matches the address *admin@test.com*.
- *admin@** – the mask matches the sender address with the *admin* name, for example, *admin@test.com*, *admin@example.org.*
- **@test** – the mask matches the address of any message sender from a domain beginning with *test*, for example: *admin@test.com*, *info@test.org.*
- *info.*@test.???* – this mask corresponds to the address of any sender whose name begins with *info.* and whose mail domain name begins with *test.* and ends with any three characters, for example: *info.product@test.com*, *info.company@test.org*, not *info.product@test.ru*.

IN THIS SECTION:

Blocked and allowed phrases 104

Obscene words 105

Blocked and allowed senders 105

Your addresses 106

Exporting and importing lists of phrases and addresses 106

BLOCKED AND ALLOWED PHRASES

You can add to the list of *blocked phrases* the expressions, which you typically observe in spam, and define the weighting coefficient for each phrase. *Weighting coefficient* allows you to specify how typical a certain phrase can be for spam messages: the larger the value, the higher the probability that mail containing such phrase is spam. Weighting coefficient of a phrase can range from 0 to 100. If the total of weighting coefficients of all phrases found in a message exceeds 100, such mail will be recognized as spam.

Key expressions typical of useful mail can be added to the list of *allowed phrases*. Once Anti-Spam finds such phrase in a message, it will be identified as useful mail (not spam).

You can add both entire phrases and their masks to the lists of blocked and allowed phrases (see section "Detecting spam by phrases and addresses. Creating lists" on page 103).

To create the list of blocked or allowed phrases:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Exact methods** tab, please do the following:
   - If you need to create a list of blocked phrases, in the **Consider message as spam** section, check the **If it contains blocked phrases** box and click the **Select** button to the right.

     The **Blocked phrases** window will open.
   - If you need to create a list of allowed phrases, in the **Consider message as not spam** section, check the **If it contains allowed phrases** box and click the **Select** button to the right.

     The **Allowed phrases** window will open.
6. Click the **Add** link to open the **Blocked phrase** window (or the **Allowed phrase** window).
7. Enter the complete phrase or expression mask, specify the weighting coefficient for a blocked phrase and then click **OK**.

You do not have to delete a mask to stop using it, unchecking the corresponding box next to it will be sufficient for the purpose.

OBSCENE WORDS

Kaspersky Lab experts have compiled the list of obscene words included into the distribution package of Kaspersky Small Office Security. The list contains obscene words that indicate a spam message with high probability, if present. You can supplement the list, adding complete phrases and their masks to it (see section "Detecting spam by phrases and addresses. Creating lists" on page 103).

To edit the list of obscene phrases:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Exact methods** tab, in the **Consider message as spam** section, check the **If it contains blocked phrases** box and click the **Select** button.

   The **Blocked phrases** window will open.
6. Check the **Consider as blocked obscene words** box and click the **obscene words** link to open the **Agreement** dialog.
7. Read the agreement and, if you agree to the terms and conditions described in the window, check the box in the bottom part of the window and click the **OK** button.

   The **Explicit language** window will open.
8. Click the **Add** link to open the **Blocked phrase** window.
9. Enter the complete phrase or its mask, specify the phrase weighting coefficient and click **OK**.

You do not have to delete a mask to stop using it, unchecking the **Explicit language** box next to it will be sufficient for the purpose.

BLOCKED AND ALLOWED SENDERS

You can add to the list of *blocked senders* the addresses, mail from which Anti-Spam will recognize as spam. Sender addresses from which you expect no spam are stored in the list of *allowed senders*. The list is created automatically during Anti-Spam training (see section "Adding an address to the list of allowed senders" on page 101). You can also supplement the list manually.

You can add to the lists of allowed or blocked senders complete addresses or address masks (see section "Detecting spam by phrases and addresses. Creating lists" on page 103).

To create the list of blocked or allowed senders:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Exact methods** tab, please do the following:

   - If you need to create a list of blocked senders, in the **Consider message as spam** section, check the **If it is from a blocked sender** box and click the **Select** button to the right.

The **Blocked senders** window will open.

- If you need to create a list of allowed senders, in the **Consider message as not spam** section, check the **If it is from an allowed sender** box and click the **Select** button to the right.

  The **Allowed senders** window opens.

6. Click the **Add** link to open the **Email address mask** window.

7. Enter an address mask and click the **OK** button.

You do not have to delete a mask to stop using it, unchecking the corresponding box next to it will be sufficient for the purpose.

YOUR ADDRESSES

You can create a list of your mail addresses to make Anti-Spam label as spam any mail that is not addressed to you directly.

To create the list of your email addresses:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Exact methods** tab, check the **If it is not addressed to me** box and click the **My addresses** button.

   The **My addresses** window opens.

6. Click the **Add** link to open the **Email address mask** window.

7. Enter an address mask and click the **OK** button.

You do not have to delete a mask to stop using it, unchecking the corresponding box next to it in **My addresses** window will be sufficient for the purpose.

EXPORTING AND IMPORTING LISTS OF PHRASES AND ADDRESSES

Having created the lists of phrases and addresses, you can reuse them, for example, transfer the addresses to a similar list on another computer running Kaspersky Small Office Security.

To do this:

1. Make *export* – copy records from the list into a file.

2. Move the file you have saved to another computer (for example, send it by email or use a removable data medium).

3. Make *import* – add the records from the file to the list of the same type on another computer.

While exporting the list, you can copy either the selected list element only, or the entire list. While importing the list, you can add the new elements to the existing list, or replace the existing list with the one being imported.

To export records from a list, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Exact methods** tab, check the box in the line containing the name of the list where the records should be exported, and click the corresponding button to the right.
6. Use the displayed list window to check the records, which should be included into the file.
7. Click the **Export** link.

   This action opens a window that offers you to export the highlighted items only. In this window, take one of the following actions:

   - click the **Yes** button if you need to include only selected records in the file;
   - click the **No** button if you need to include the entire list in the file.
8. Specify in the displayed window the type and name for the file and confirm its saving.

To import records from file to a list, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Exact methods** tab, check the box in the line containing the name of the list where the records should be imported, and click the button to the right.
6. Click the **Import** link in the list window. If you are importing a list of allowed senders, the application will display a menu where you should select the **Import from file** item. For other list types selection from the menu is not required.

   If the list is not empty, a window opens offering you to add items to be imported. In this window, take one of the following actions:

   - click the **Yes** button if you want to add records from the file into the list;
   - click the **No** button if you want to replace the existing records with the list from the file.
7. In the window that opens, select the file with the list of records that you want to import.

Importing the list of allowed senders from address book

Addresses in the list of allowed senders can be imported from Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail) address books.

To import the list of allowed senders from an address book, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Exact methods** tab, in the **Consider message as not spam** block, check the **If it is from an allowed sender** box and click the **Select** button.

   The **Allowed senders** window opens.

6. Click the **Import** link, open the source selection menu, and select **Import from the Address Book**.

7. Use the window that opens to select the necessary address book.

REGULATING THRESHOLD VALUES OF SPAM RATE

Spam recognition is based on cutting-edge filtering methods, which allow you to train (see section "Training Anti-Spam" on page 99) Anti-Spam to distinguish spam, probable spam and useful email. In doing so, every individual element of good emails or spam is assigned a factor.

When an email message enters your inbox, Anti-Spam scans the message using the iBayes algorithm for elements of spam and good email. The component sums up the ratings of each spam (useful mail) item and calculates the resulting *spam rate*. The larger the spam rate, the higher the probability that such mail contains spam. A message is recognized by default as useful mail if its spam rate does not exceed 60. If spam rate is higher than 60, such message is considered to be potential spam. If the value exceeds 90, such message is recognized as spam. You can modify the threshold values for the spam rate.

To change the spam rate thresholds, perform the following steps:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Expert methods** tab, use the **Spam rate** section to configure the spam rate values using the corresponding sliders or entry fields.

USING ADDITIONAL SPAM FILTERING FEATURES

The result of spam rate calculation can be affected by additional message characteristics, for example, a missing recipient's address in the "To" field or a very long message subject (over 250 characters). When present in a message, such signs increase the probability of its being spam. Consequently, the spam rate will grow. You can select the additional signs that will be taken into account during message analysis.

To use additional signs increasing the spam rate, perform the following steps:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

4. Click the **Settings** button in the **Security level** section in the right part of the window.

5. In the window that opens, on the **Expert methods** tab, click the **Additional** button.

6. In the displayed **Additional** window, check the boxes next to the signs, which should be taken into account during message analysis increasing the spam rate.

SELECTING THE SPAM RECOGNITION ALGORITHM

The Anti-Spam mail analysis is based on the selected recognition algorithms:

- **Heuristic Analysis**. Anti-Spam analyzes messages using heuristic rules. Heuristic analysis is always enabled.
- **Image recognition (GSG technology)**. Anti-Spam uses GSG technology to detect graphic spam.
- **Analysis of attachments in .rtf format**. Anti-Spam analyzes documents attached to messages checking them for spam signs.
- **Self-training text recognition algorithm (iBayes)**. Operation of the iBayes algorithm is based on the analysis calculating the frequency of words typical for spam in the text of the analyzed mail. The analysis identifies each message as useful mail or spam. To start using the iBayes algorithm, you should train Anti-Spam (see section "Training Anti-Spam" on page 99).

To enable / disable a specific spam recognition algorithm for analysis of email messages:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Expert methods** tab, in the **Recognition algorithms** block, check or uncheck the corresponding boxes.

ADDING A LABEL TO THE MESSAGE SUBJECT

Anti-Spam can add appropriate labels to the **Subject** field of the message recognized after analysis as spam or potential spam:

- **[!! SPAM]** – for messages identified as spam.
- **[?? Probable Spam]** – for messages identified as potential spam.

When present in message subject, such labels can help you distinguish spam and probable spam visually while viewing the mail lists.

To enable / disable addition of labels to the message subjects by Anti-Spam:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Additional** tab, in the **Actions** section, check the boxes next to the labels, which should be added to message subject. Having checked the box, you can modify the associated label text. To prevent label addition, uncheck its corresponding box.

FILTERING EMAIL MESSAGES AT THE SERVER. MAIL DISPATCHER

You can view the list of email messages on the server without downloading them to your computer. The opportunity allows you to reject some messages saving time and traffic while working with email and also decreasing the risk of downloading spam or viruses to your computer.

Mail Dispatcher is used to manage the messages residing on the server.

The Mail Dispatcher window opens every time before mail retrieval provided that it is enabled.

Note that Mail Dispatcher opens only when mail is received via POP3 protocol. Mail Dispatcher does not appear if your POP3 server does not support viewing email headers or if all messages on the server are sent from the addresses included into the list of allowed senders (see page 105).

The list of email messages residing on the server is displayed in the central part of the Mail Dispatcher window. Select the message in the list for a detailed analysis of its header.

Header viewing may be useful, for example, in this situation: spammers install a malicious program on your colleague's computer; this program sends spam with his name on it, using his mail client's contact list. The probability that your address is present in the contact list of your colleague is quite high; consequently, malware can send lots of spam messages to your mailbox.

In such cases the sender address alone is insufficient to determine if a message has been sent by your colleague or spammer malware. Message header provides more details: who sent the letter and when, its size, route from the sender to your mail server. This information allows you to decide if a message really should be downloaded from the server or if it is safer to delete it.

To use Mail Dispatcher:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Additional** tab, in the **Incoming messages** block, check the **Open Mail Dispatcher when receiving email through POP3 protocol** box.

To delete messages from the server using Mail Dispatcher:

1. In the Mail Dispatcher window, which opens before the message is received, check the box next to this message in the **Delete** column.
2. Click the **Delete selected** button in the top part of the window.

Messages will be deleted from the server. You will receive a notification marked as **[!! SPAM]** and processed according to the rules set for your mail client (see section "Configuring spam processing by mail clients" on page 111).

EXCLUDING MICROSOFT EXCHANGE SERVER MESSAGES FROM THE SCAN

You can exclude from anti-spam scanning email messages which originate within the internal network (for example, corporate mail). Please note that messages are considered internal mail if Microsoft Office Outlook is used on all network computers and user mailboxes are located on the same Exchange server or on servers linked via X400 connectors.

By default, the Anti-Spam component does not scan Microsoft Exchange Server messages.

If you wish Anti-Spam to analyze the messages transferred via Microsoft Exchange Server, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. Click the **Settings** button in the **Security level** section in the right part of the window.
5. In the window that opens, on the **Additional** tab, in the **Exclusions** block, uncheck the **Do not check Microsoft Exchange Server native messages** box.

CONFIGURING SPAM PROCESSING BY MAIL CLIENTS

If after scanning you find that an email is spam or probable spam, further actions of Anti-Spam depend on the status of the message and the action selected. By default, email messages considered spam or probable spam, are modified: in the **Subject** field of the message, the label **[!! SPAM]** or **[?? Probable Spam]** is added, respectively (see section "Adding a label to the message subject" on page 109).

You can select additional actions to be taken on spam or probable spam. To do so, special plug-ins are provided in the Microsoft Office Outlook and Microsoft Outlook Express (Windows Mail) clients. You can configure filtration rules for The Bat! and Thunderbird email clients.

IN THIS SECTION:

Microsoft Office Outlook 111

Microsoft Outlook Express (Windows Mail) 111

Creating the rule for handling spam reports 112

The Bat! 112

Thunderbird 113

MICROSOFT OFFICE OUTLOOK

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field. If additional mail processing after Anti-Spam checks is required, you can configure Microsoft Office Outlook as necessary. The spam processing settings window automatically opens the first time you run Microsoft Outlook after installing Kaspersky Small Office Security. The spam and probable spam processing settings for Microsoft Outlook are displayed on the special **Anti-Spam** tab of the **Tools** → **Options** menu item.

MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field. If additional mail processing after Anti-Spam checks is required, you can configure Microsoft Outlook Express (Windows Mail) as necessary.

The spam processing settings window opens when you run your client after the installation of the application. You can also open it by clicking the **Settings** button in the e-mail client toolbar next to the **Spam** and **Not Spam** buttons.

CREATING THE RULE FOR HANDLING SPAM REPORTS

Below are the instructions for creating the rule for handling spam reports using Anti-Spam in Microsoft Office Outlook. You can use the guidelines to create custom rules.

To create a spam processing rule:

1. Run Microsoft Office Outlook and use the **Tools** → **Rules and Alerts** command in the main application menu. The method used to access the wizard depends upon your version of Microsoft Office Outlook. This Help file describes how to create a rule using Microsoft Office Outlook 2003.

2. In the **Rules and Alerts** window that opens, on the **Email Rules** tab click the **New Rule** button. As a result, the Rules Wizard is launched. The Rules Wizard includes the following steps:

   a. You should decide whether you want to create a rule from scratch or use a template. Select the **Start from a blank rule** option and select the **Check messages when they arrive** scan condition. Click the **Next** button.

   b. Click the **Next** button in the message filtering condition configuration window without checking any boxes. Confirm in the dialog box that you want to apply this rule to all emails received.

   c. In the window for selecting actions in respect to messages, check the **perform a custom action** box in the action list. In the lower part of the window, click the **a custom action** link. Select **Kaspersky Anti-Spam** from the drop-down list in the window that opens and click the **OK** button.

   d. Click the **Next** button in the exclusions from the rules window without checking any boxes.

   e. In the final window, you can change the rule's name (the default name is Kaspersky Anti-Spam). Make sure that the **Turn on this rule** box is checked, and click the **Finish** button.

3. The default position for the new rule is first on the rule list in the **Rules and Alerts** window. If you like, move this rule to the end of the list so it is applied to the email last.

All incoming emails are processed with these rules. The order in which rules are applied depends upon the priority specified for each rule. Rules are applied from the list beginning; the priority of each following rule is lower than that of the preceding one. You can increase or decrease rule priority moving a rule up or down in the list. If you do not want the Anti-Spam rule to further process emails after a rule is applied, you must check the **Stop processing more rules** box in the rule settings (see Step 3 in creating a rule).

THE BAT!

Actions in respect of spam and probable spam in The Bat! are defined by the client's own tools.

To modify spam processing rules in The Bat!:

1. Select the **Settings** item from the **Properties** menu of the mail client.

2. Select the **Spam protection** object from the settings tree.

Displayed settings of anti-spam protection apply to all installed Anti-Spam modules that support integration with The Bat!.

You need to define the rating level and specify how messages with certain a rating should be handled (in case of Anti-Spam – the probability of message being spam):

- delete messages with the rating that exceeds the specified value;
- move email messages with a given rating to a special spam folder;
- move spam marked with special headers to the spam folder;

- leave spam in the **Inbox** folder.

After processing an email, Kaspersky Small Office Security assigns a spam or probable spam status to the message based on a rating with an adjustable value. The Bat! has its own email rating algorithm for spam, also based on a spam rate. To prevent discrepancies between spam rate in Kaspersky Small Office Security and The Bat!, all messages checked in Anti-Spam are assigned the rating corresponding to the message status: Not Spam email – 0%, Probable spam – 50%, Spam – 100%. Thus, the email rating in The Bat! corresponds to the rating of the relevant status and not to the spam rate assigned in Anti-Spam.

For more details on the spam rate and processing rules, see the documentation for The Bat! mail client.

THUNDERBIRD

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field. If additional mail processing after Anti-Spam checks is required, you can configure Thunderbird having opened its configuration window from the **Tools** → **Message Filters** menu (for more details about using the mail client see Mozilla Thunderbird Help).

Thunderbird's Anti-Spam plug-in module allows training based on messages received and sent using this email client application and checking your email correspondence for spam on the server. The plug-in module is integrated into Thunderbird and forwards messages to the Anti-Spam component for scanning when commands from the **Tools** → **Run anti-spam filters** in folder menu are being executed. As such, Kaspersky Small Office Security checks messages instead of Thunderbird. This does not alter the functionality of Thunderbird.

The Anti-Spam plug-in module status is displayed as an icon in the Thunderbird status line. The gray color of the icon informs the user that there is a problem in the plug-in operation or that the Anti-Spam component is disabled. Double-click the icon to open the settings of Kaspersky Small Office Security. To modify the Anti-Spam settings, click the **Settings** button in the **Anti-Spam** section.

ANTI-BANNER

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Anti-Banner is designed to block banners on web pages you open and those in the interface of specified applications. Ads on banners may distract you from your business activity while banner downloads increase the amount of inbound traffic.

Before a banner is displayed on a web page or in an application's window, it should be downloaded from the Internet. Anti-Banner scans the address from which the banner is downloaded. If the address is associated to a mask from the list included with the Kaspersky Small Office Security package, or from the list of blocked banners addresses you have compiled on your own, Anti-Banner blocks the banner. To block banners with address masks not found in the mentioned lists, the heuristic analyzer is used.

Additionally, you can create a list of allowed addresses to determine which banners should be allowed for display.

IN THIS SECTION:

Enabling and disabling Anti-Banner 114

Selecting the scan method 114

Creating the lists of blocked and allowed banner addresses 114

Exporting and importing the lists of addresses 115

ENABLING AND DISABLING ANTI-BANNER

By default, Anti-Banner is enabled, functioning in normal mode. You can disable Anti-Banner, if necessary.

To enable or disable Anti-Banner, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
4. In the right part of the window, uncheck the **Enable Anti-Banner** box if you need to disable this component. Check this box if you need to enable the component.

SELECTING THE SCAN METHOD

You can specify which methods should be used by Anti-Banner to scan addresses from which banners may be downloaded. In addition to these methods, Anti-Banner checks banner addresses for compliance to the masks from the lists of allowed and blocked addresses if those are in use.

To select methods of address scan by Anti-Banner:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
4. In the right part of the window, in the **Scan methods** group, check the boxes next to the names of the methods that should be used.

CREATING THE LISTS OF BLOCKED AND ALLOWED BANNER ADDRESSES

Using the lists of blocked and allowed banners addresses, you can allow banners to be downloaded for a specified group of addresses and block them for another group. Create a list of blocked address masks to let Anti-Banner block download and display of banners from the addresses that correspond to those masks. Create a list of allowed address masks to let Anti-Banner download and display banners from the addresses that correspond to those masks.

To add a mask to the list of blocked (allowed) addresses:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
4. In the right part of the window, in the **Additional** section, check the **Use the list of blocked URLs** box (or the **Use the list of allowed URLs** box) and click the **Settings** button located under the box.

   The **Blocked URLs** (or **Allowed URLs**) window opens.
5. Click the **Add** link to open the **Address mask (URL)** window.
6. Enter a blocked (or allowed) banner mask and click the **OK** button.

You do not have to delete a mask to stop using it, unchecking the corresponding box next to it will be sufficient for the purpose.

EXPORTING AND IMPORTING THE LISTS OF ADDRESSES

After you have created the lists of allowed or blocked banner addresses, you can use them repeatedly: for example, export banner addresses to a similar list on another computer with Kaspersky Small Office Security installed on it.

To do this:

1. Make *export* – copy records from the list into a file.
2. Move the file you have saved to another computer (for example, send it by email or use a removable data medium).
3. Make *import* – add the records from the file to the list of the same type on another computer.

While exporting the list, you can copy either the selected list element only, or the entire list. While importing the list, you can add the new elements to the existing list, or replace the existing list with the one being imported.

To export banner addresses from the list of allowed or blocked URLs, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
4. In the right part of the window, in the **Additional** section, click the **Settings** button located in the line with the name of the list from which you should copy addresses into a file.
5. In the **Blocked URLs** (or **Allowed URLs**) window that opens, check the boxes next to the addresses that you need to include in the file.
6. Click the **Export** button.

   This action opens a window that offers you to export the highlighted items only. In this window, take one of the following actions:

   - click the **Yes** button if you need to include only selected addresses in the file;
   - click the **No** button if you need to include the entire list in the file.
7. In the window that opens, enter a name for the file you want to save and confirm saving.

To import banner addresses from a file to the list of allowed or blocked URLs, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
4. In the right part of the window, in the **Additional** section, click the **Settings** button located in the line with the name of the list into which you need to add addresses from a file.
5. In the **Blocked URLs** (or **Allowed URLs**) window that opens, click the **Import** button.

   If the list is not empty, a window opens offering you to add items to be imported. In this window, take one of the following actions:

- click the **Yes** button if you want to add records from the file into the list;
- click the **No** button if you want to replace the existing records with the list from the file.

6. In the window that opens, select the file with the list of records that you want to import.

SECURITY ZONE

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Security Zone prevents applications from performing actions that may be dangerous for the system, and ensures control of access to operating system resources and your identity data.

The component tracks actions in the system performed by applications installed on the computer, and regulates them based on the rules of Security Zone. These rules regulate potentially dangerous activity, including applications' access to protected resources, such as files and folders, registry keys, and network addresses.

Network activity of the applications is controlled by the Firewall component.

At the first startup of an application on the computer, the Security Zone component verifies its safety and includes it into one of the trust groups. The trust group defines the rules that Kaspersky Small Office Security should apply to control the activity of this application. Rules of Security Zone is a set of rights of access to the computer resources and restrictions posed on various actions being performed by applications on the computer.

You can configure the conditions for distribution of applications by groups (see page 117), move an application to another group (see page 119), or edit the rules of Kaspersky Small Office Security (see page 119).

We recommend that you participate in Kaspersky Security Network (see section "Participating in Kaspersky Security Network" on page 224) in order to improve performance of Security Zone. Data obtained using Kaspersky Security Network allow you to distribute applications by groups with more accuracy and apply optimum rules of Security Zone.

When the application is restarted, the Security Zone component checks its integrity. If the application has not been changed, the component applies the current rule to it. If the application has been modified, the Security Zone component re-scans it as at the first startup.

To control applications' access to various resources of your computer, you can use the preset list of protected resources or add user resources to the list (see page 123).

IN THIS SECTION:

Enabling and disabling Security Zone 117

Placing applications into groups 117

Viewing activity of applications 118

Modifying a trust group 119

Security Zone rules 119

Protecting operating system resources and identity data 123

ENABLING AND DISABLING SECURITY ZONE

By default, Security Zone is enabled, functioning in the mode developed by Kaspersky Lab specialists. However, you can disable it, if required.

To enable or disable Security Zone, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Security Zone** component.
4. In the right part of the window, uncheck the **Enable Security Zone** box if you need to disable this component. Check this box if you need to enable the component.

PLACING APPLICATIONS INTO GROUPS

At the first startup of an application on the computer, the Security Zone component verifies its safety and includes it into one of the trust groups.

At the first stage of the application scan, Kaspersky Small Office Security searches the internal database of known applications for a matching entry, and then sends a request to the Kaspersky Security Network database (if an Internet connection is available). If an entry of that application is found in the database, the application is included into a group registered in the database.

Applications that do not pose any threat to the system are included into the **Trusted** group. By default, this group includes applications with a digital signature and applications whose parent objects have one.

You can disable the automatic inclusion of applications contained in the Kaspersky Security Network database or having a digital signature into the **Trusted** group.

Behavior of applications included into the **Trusted** group will however be controlled by the Proactive Defense component.

By default, Kaspersky Small Office Security uses the heuristic analysis to distribute unknown applications (not included into the Kaspersky Security Network database and functioning without a digital signature) by groups. The analysis helps defining the threat rating of the application based on which it is included into a group. Instead of using the heuristic analysis, you can specify a group into which Kaspersky Small Office Security should automatically include all unknown applications.

By default, Security Zone analyzes an application for 30 seconds. If this time interval turns out to be insufficient for defining the threat rating, the application is included into the **Low restricted** group, while defining the threat rating continues in background mode. After that, the application is finally included into another group. You can change the time allocated for application analysis. If you are sure that all applications started on your computer do not pose any threat to its security, you can decrease the time spent on analysis. If, on the contrary, you are installing the software and are not sure that this is safe, you are advised to increase the time for analysis.

If the application threat rating is high, Kaspersky Small Office Security notifies you about it and offers you to select a group where to place the application. Notification contains statistics of the application use by Kaspersky Security Network participants. Based on the statistics and with regard for the history of emergence of this application on your computer, you can make a weighed decision on the group into which the application should be included.

*To disable the automatic inclusion of applications contained in the Kaspersky Security Network database or having a digital signature into the **Trusted** group,*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Security Zone** component.

4. In the right part of the window, in the **Trusted applications** section, uncheck the **Applications with digital signature** and **Trusted in Kaspersky Security Network database** boxes.

To use the heuristic analysis for distributing unknown applications by groups:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Security Zone** component.

4. In the right part of the window, in the **Trusted applications** section, select **Use the heuristic analysis to define group**.

To change the time allowed for calculation of the application group:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Security Zone** component.

4. In the right part of the window, in the **Additional** section, edit the value of the **Maximum time to define the application group** setting.

To include all unknown applications into the specified group:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Security Zone** component.

4. In the right part of the window, in the **Trusted applications** section, select **Move to the following group automatically** and specify the required group from the dropdown list.

VIEWING ACTIVITY OF APPLICATIONS

You can view information about all applications being used on your computer and all processes being currently run.

To view applications' activity:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. Follow the **Applications Activity** link in the right part of the window.
4. In the **Application activity** window that opens, in the **Category** list, select the required application category.

MODIFYING A TRUST GROUP

At the first startup of an application, Kaspersky Small Office Security automatically includes it into a group (see section "Placing applications into groups" on page 117). If necessary, you can move the application to another group manually.

Kaspersky Lab specialists recommend that you avoid moving applications from default groups. Instead, if required, edit the rules for an individual application (see section "Editing application rules" on page 120).

To move an application to another group:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. Follow the **Applications Activity** link in the right part of the window.
4. In the **Application activity** window that opens, in the **Category** list, select the required application category.
5. Right-click to open the context menu of the required application and select **Move to group** → **<group name>**.

To move the application to the default group, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. Follow the **Applications Activity** link in the right part of the window.
4. In the **Application activity** window that opens, in the **Category** list, select the required application category.
5. Right-click to open the context menu for the required application and select **Move to group** → **Restore default group**.

SECURITY ZONE RULES

Rules of Security Zone is a set of rights of access to the computer resources and restrictions posed on various actions being performed by applications on the computer.

By default, an application is controlled according to the rules of the trust group into which Kaspersky Small Office Security included the application when it was run for the first time. Group rules have been developed by Kaspersky Lab specialists for an optimum control of applications' activity. If necessary, you can edit these rules or adjust them for an individual application. Rules of an application have a higher priority than rules of a group.

IN THIS SECTION:

Editing group rules 120

Editing application rules 120

Creating a network rule for application 121

Configuring exclusions 121

Inheritance of restrictions of the parent process 122

Deleting rules for applications 122

EDITING GROUP RULES

By default, different trust groups have different optimum sets of rights of access to the computer resources. You can edit the preset group rules.

To change the group rule:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Security Zone** component.
4. Click the **Configure rules** button in the right part of the window.
5. In the **Rules for application groups** window that opens, select the required group.
6. Click the **Change** link to open the **Rules for a group of applications** window.
7. On the **Rules** tab, edit the access rules for the required resource category.

EDITING APPLICATION RULES

When an application is started for the first time, Security Zone determines its status and includes it in a certain group. After that, the component logs the actions performed by this application in the system, and manages its activity based on which group it belongs to. When an application accesses a resource, the component checks if the application has the required access rights, and performs the action determined by the rule. You can edit the rule that was created for the application when determining its status and including the application in the corresponding group.

To change an application rule:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. Follow the **Applications Activity** link in the right part of the window.
4. In the **Application activity** window that opens, in the **Category** list, select the required application category.
5. In the **Group** column, left-click the link with the name of the group for the required application.
6. In the menu that opens, select **Move to group** → **Custom settings**.
7. In the window that opens, on the **Rules** tab, edit the access rules for the required resource category.

CREATING A NETWORK RULE FOR APPLICATION

If you need to process the application's access to certain network services in a special way, you can create a network rule.

To create a rule controlling the application's network activity, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. Follow the **Applications Activity** link in the right part of the window.
4. In the **Application activity** window that opens, in the **Category** list, select the required application category.
5. In the **Group** column, left-click the link with the name of the group for the required application.
6. In the menu that opens, select **Move to group** → **Custom settings**.
7. In the window that opens, on the **Rules** tab, select the **Network rules** category from the dropdown list, and click the **Add** link.
8. In the **Network rule** window that opens, configure the network rule.
9. Assign a priority to the new rule by moving it up or down the list clicking the **Move up** and **Move down** buttons.

   Once you have created the rule, you can modify its settings or delete it using buttons in the top part of the tab. To disable the rule, uncheck the box next to the rule's name.

CONFIGURING EXCLUSIONS

When you create a default application rule, Kaspersky Small Office Security will monitor any of the user application's actions, including: access to files and folders, access to the execution environment, and network access. You can exclude certain actions of a user application from the scan.

In order to exclude applications' actions from the scan:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. Follow the **Applications Activity** link in the right part of the window.
4. In the **Application activity** window that opens, in the **Category** list, select the required application category.
5. In the **Group** column, left-click the link with the name of the group for the required application.
6. In the menu that opens, select **Move to group** → **Custom settings**.
7. In the window that opens, on the **Exclusions** tab, check the boxes that match the actions you wish to exclude. When excluding the application's network traffic from the scan, configure additional exclusion settings.

   All exclusions created in the rules for user applications are accessible in the application settings window in the **Threats and exclusions** section.

INHERITANCE OF RESTRICTIONS OF THE PARENT PROCESS

Application startup may be initiated either by the user or by another application running. If the startup is initiated by another application, it creates a startup procedure including parent and child applications.

When an application attempts to obtain access to a protected resource, Security Zone analyzes the rights of all parent processes of this application, and compares them to the rights required to access this resource. The minimum priority rule is then observed: when comparing the access rights of the application to those of the parent process, the access rights with a minimum priority will be applied to the application's activity.

Access right priority:

1. Allow. Access right data has the highest priority.
2. Prompt user.
3. Block. Access right data has the lowest priority.

This mechanism prevents a non-trusted application or an application with restricted rights from using a trusted application to perform actions requiring certain privileges.

If an application's activity is blocked because a parent process has insufficient rights, you can edit these rules (see section "Editing application rules" on page 120) or disable inheritance of restrictions from the parent process.

You should modify the rights of a parent process only if you are absolutely certain that the process' activities do not threaten the security of the system.

To disable inheritance of restrictions from the parent process, perform the following steps:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. Follow the **Applications Activity** link in the right part of the window.
4. In the **Application activity** window that opens, in the **Category** list, select the required application category.
5. In the **Group** column, left-click the link with the name of the group for the required application.
6. In the menu that opens, select **Move to group** → **Custom settings**.
7. On the **Rules** tab of the displayed window, uncheck the **Inherit restrictions of the parent process (application)** box.

DELETING RULES FOR APPLICATIONS

By default, the rules for applications which have not been started for the 60 days are deleted automatically. You can modify the storage time for rules for unused applications, or disable rules' automatic removal.

To set the storage time for application rules:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that opens, in the **Protection Center** section, select the **Security Zone** component.
3. For the selected component, check the **Delete rules for applications remaining inactive for more than** box in the **Additional** section and specify the necessary number of days.

To disable the automatic removal of the rules for unused applications:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that opens, in the **Protection Center** section, select the **Security Zone** component.
3. In the **Additional** section, uncheck the **Delete rules for applications remaining inactive for more than** box for the selected component.

PROTECTING OPERATING SYSTEM RESOURCES AND IDENTITY DATA

Security Zone manages the applications' rights to take actions on various resource categories of the operating system and identity data.

Kaspersky Lab specialists have distinguished the preset categories of protected resources. You cannot edit this list. However, you can expand this list by adding user categories and / or individual resources, or stop controlling the selected resources.

To add identity data to be protected:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that opens, in the **Protection Center** section, select the **Security Zone** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that opens, on the **Identity data** tab, in the **Category** dropdown list, select the required category of identity data and open the window for adding resources, by clicking the **Add** link.
5. In the **User resource** window that opens, click the **Browse** button and specify required data, depending on the resource being added.

After you add a resource, you can edit or remove it using the respective buttons in the top part of the tab. To disable the control of a resource or category, uncheck the box next to it.

To create the category of identity data items to be protected:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that opens, in the **Protection Center** section, select the **Security Zone** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that opens, on the **Identity data** tab, open the window for adding resources, by clicking the **Add category** link.
5. In the **Identity data category** window that opens, enter a name for the new resource category.

To add operating system settings and resources to be protected:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that opens, in the **Protection Center** section, select the **Security Zone** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that opens, on the **Operating system** tab, in the **Category** dropdown list, select the required category of operating system objects and open the window for adding resources, by clicking the **Add** link.

After you add a resource, you can edit or remove it using the respective buttons in the top part of the tab. To disable the control of a resource or category, uncheck the box next to it.

PROACTIVE DEFENSE

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Proactive Defense ensures protection against new threats which are not yet included in Kaspersky Small Office Security databases.

The preventative technologies provided by Proactive Defense neutralize new threats before they harm your computer. In contrast with responsive technologies, which analyze code based on records in Kaspersky Small Office Security databases, preventative technologies recognize a new threat on your computer by the sequence of actions executed by a program. If, as a result of activity analysis, the sequence of an application's actions arouses suspicion, Kaspersky Small Office Security blocks the activity of this application.

For example, when actions such as a program copying itself to network resources, the startup folder and the system registry are detected, it is highly likely that this program is a worm. Hazardous sequences of actions also include attempts to modify the HOSTS file, hidden installation of drivers, etc. You can turn off monitoring for any hazardous activity or edit the rules of monitoring (see page 125) for it.

As opposed to the Security Zone, Proactive Defense responds immediately to a defined sequence of an application's actions. Activity analysis is performed for all applications, including those grouped as **Trusted** by the Security Zone component.

You can create a group of trusted applications (see page 125) for Proactive Defense. If done, you will not be notified of activities of these applications.

If your computer runs under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7, or Microsoft Windows 7 x64, control will not apply to each event. This is due to specific features of these operating systems. For example, control will not apply in full volume to the sending data through trusted applications, and suspicious system activities.

IN THIS SECTION:

Enabling and disabling Proactive Defense 124

Creating a group of trusted applications 125

Using the dangerous activity list 125

Changing the dangerous activity monitoring rule 125

Rolling back a malicious program's actions 126

ENABLING AND DISABLING PROACTIVE DEFENSE

By default, Proactive Defense is enabled, functioning in optimum mode. You can disable Proactive Defense, if required.

To enable or disable Proactive Defense, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.

4. In the right part of the window, uncheck the **Enable Proactive Defense** box if you need to disable this component. Check this box if you need to enable the component.

CREATING A GROUP OF TRUSTED APPLICATIONS

Programs recognized by the Security Zone component as **Trusted** pose no threat for the system. However, their activities will also be monitored by Proactive Defense.

You can create a group of trusted applications; Proactive Defense will not monitor their activity. By default, the list of trusted applications includes applications with verified digital signature and applications from Kaspersky Security Network database.

To change the settings of the trusted applications group, perform the following steps:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.

4. In the right part of the window, in the **Trusted applications** section, check the boxes next to the required settings.

USING THE DANGEROUS ACTIVITY LIST

The list of actions typical of dangerous activity cannot be edited. You can turn off monitoring for one dangerous activity or another.

To turn off monitoring for one dangerous activity or another:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.

4. Click the **Settings** button in the right part of the window.

5. In the **Proactive Defense** window that opens, uncheck the box next to the type of activity which you do not want to be monitored.

CHANGING THE DANGEROUS ACTIVITY MONITORING RULE

Applications' actions classified as dangerous activity cannot be edited. You can perform the following actions:

- turn off monitoring for any activity (see page 125);
- create an exclusion list, by listing applications the activities of which you do not consider dangerous;
- edit the rule that Proactive Defense uses when it detects dangerous activity.

To change the rule:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
4. Click the **Settings** button in the right part of the window.
5. In the **Proactive Defense** window that opens, in the **Event** column, select the required event for which you want to edit the rule.
6. Configure the settings for the selected event using the links in the **Rule description** section. For example:
   a. Click the link with the preset action and select the required action in the **Select action** window that opens.
   b. Click the link with the preset time period (not for any activity type), and in the **Hidden processes detection** window that opens, specify the scan interval for hidden processes.
   c. Click the **On / Off** link to indicate that a report on operation execution should be created.

ROLLING BACK A MALICIOUS PROGRAM'S ACTIONS

Proactive Defense allows rolling back of a malicious activity in the system.

By default, during the Kaspersky Small Office Security operation in automatic mode, the rollback of malware actions is performed automatically upon detection of a malicious activity by the Proactive Defense component. When working in interactive mode (see page 39), you can change the action to be performed upon detection of a malicious activity.

The procedure of rolling back malware operations affects a defined set of data. It causes no negative consequences for the operating system or data integrity on your computer.

To configure rollback of malware operations, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
4. In the right part of the window, in the **Additional** section, select the required response to malware actions.

NETWORK PROTECTION

Various protection components, tools, and settings of Kaspersky Small Office Security together ensure security and control of your network activities.

The sections below contain detailed information about the principles of operation and configuration of Firewall, Network Attack Blocker, Network Monitor, scan of secure connections, proxy server settings, and monitoring of network ports.

IN THIS SECTION:

Firewall 127

Network Attack Blocker 130

Encrypted connections scan 133

Network Monitor 135

Configuring the proxy server 135

Creating a list of monitored ports 135

FIREWALL

The Firewall ensures security for your work in local networks and on the Internet.

The component filters the entire network activity according to the network rules of Security Zone. Network rule is an action that Firewall performs when it detects a connection attempt that has a specified status. Status is assigned to each network connection; it is defined by specified settings: data transfer direction and protocol, addresses and ports to which the connection is established.

The Firewall analyzes the settings of the networks to which you connect your computer. If the application works in interactive mode, the Firewall, when first connected, will request that you specify a status of the connected network. If interactive mode is off, the Firewall defines the status based on the network type, ranges of addresses and other specifications. You can change the status of the network connection manually.

In Kaspersky Small Office Security 2 for File Server, the Firewall is disabled by default.

IN THIS SECTION:

Enabling and disabling Firewall 127

Changing the network status 128

Extending the range of network addresses 128

Working with Firewall rules 128

Configuring notifications of changes in the network 130

Advanced Firewall settings 130

ENABLING AND DISABLING FIREWALL

By default, the Firewall is enabled, functioning in normal mode. You can disable the Firewall if needed.

To enable or disable the Firewall, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.

4. In the right part of the window, uncheck the **Enable Firewall** box if you need to disable this component. Check this box if you need to enable the component.

CHANGING THE NETWORK STATUS

The network connection status affects the set of rules used to filter network activity for that connection. You can change the network status, if necessary.

To change the network connection status:

1. Open the main application window and click the **Settings** link in the top part.

2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.

3. Click the **Settings** button for the component you have selected.

4. In the window that opens, on the **Networks** tab, select an active network connection and click the **Edit** link.

5. In the window that opens, select the required status from the drop-down list on the **Properties** tab.

EXTENDING THE RANGE OF NETWORK ADDRESSES

Each network matches one or more ranges of IP address. If you connect to a network, access to subnetwork of which is performed via a router, you can manually add subnetworks accessible through it.

Example:

You are connecting to the network in an office of your company and wish to use the same filtering rules for the office where you are connected directly and for the offices accessible over the network.

Obtain network address ranges for those offices from the network administrator and add them.

To extend the range of network addresses:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.

3. Click the **Settings** button for the component you have selected.

4. In the window that opens, on the **Networks** tab, select an active network connection and click the **Edit** link.

5. In the window that opens, on the **Properties** tab, in the **Additional subnetworks** block, click the **Add** link.

6. In the **IP address** window that opens, specify an IP address or an address mask.

WORKING WITH FIREWALL RULES

The Firewall operates on the basis of two types of rules:

- *Packet rules.* They are used for posing restrictions on packets regardless of the application. Typically, such rules restrict incoming network activity on specified TCP and UDP ports and filter ICMP messages.

- *Application rules*. They are used to set limits on network activity of a specified application. Such rules allow fine-tuning the activity filtering, for example, when a certain type of network connections is banned for some applications but is allowed for others.

Packet rules have higher priority than application rules. If both packet rules and rules for applications are applied to the same type of network activity, this network activity is processed using the packet rules. Besides, you can set a priority for each rule.

CREATING A PACKET RULE

Packet rules consist of a set of conditions and operations over packets performed when these conditions are met.

When creating packet rules, remember that they have priority over the rules for applications.

To create a packet rule:

1. Open the main application window and click the **Settings** link in the top part.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that opens, on the **Filtering rules** tab, select the **Packet rules** block and click the **Add** link.
5. In the **Network rule** window that opens, specify the required settings and click the **OK** button.
6. Assign a priority to the new rule by moving it up or down the list using the **Move up** and **Move down** links.

   After you have created the rule, you can modify its settings or delete it using links in the bottom part of the tab. To disable the rule, uncheck the box next to the rule's name.

EDITING GROUP RULES

Similarly to the Security Zone component, Firewall's default feature is to filter network activity of an application using the rules of the group in which this application has been included.

Network rules of a trust group define which rights of access to various networks can be granted to the applications that have been included in this group. You can edit the preset network rules of a group.

To change a network rule for a group:

1. Open the main application window and click the **Settings** link in the top part.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Configure rules** button for the chosen component.
4. In the window that opens, select a group, right-click to open the context menu and choose the required option: **Allow**, **Deny** or **Prompt for action**.

EDITING APPLICATION RULES

You can create network rules for individual applications. Network rules of an application have a higher priority than network rules of a group.

If necessary, you can create network rules for applications (see page 121) using the Security Zone component.

To create an application rule, please do the following:

1. Open the main application window and click the **Settings** link in the top part.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that opens, on the **Filtering rules** tab, select the group of rules for an application and click the **Add** link.
5. In the **Network rule** window that opens, configure the network rule.
6. Assign a priority to the new rule by moving it up or down the list using the **Move up** and **Move down** links.

   After you have created the rule, you can modify its settings or delete it using links in the bottom part of the tab. To disable the rule, uncheck the box next to the rule's name.

CONFIGURING NOTIFICATIONS OF CHANGES IN THE NETWORK

Network connection settings can be changed during operation. You can receive notifications of modifications in the settings.

To enable notification about changes to network connection settings:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that opens, on the **Networks** tab, select an active network connection and click the **Edit** link.
5. In the window that opens, check the boxes for those events about which you wish to receive notifications on the **Additional** tab.

ADVANCED FIREWALL SETTINGS

You can specify the advanced settings for the Firewall, such as permission of FTP's active mode, connection blockage if no prompt for action is available (application interface is not loaded), and functioning until the system shutdown.

By default, all the settings are enabled.

To modify advanced settings of the Firewall:

1. Open the main application window and click the **Settings** link in the top part.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that opens, on the **Filtering rules** tab, click the **Additional** button.
5. In the **Additional** window that opens, check / uncheck the boxes next to the required settings.

NETWORK ATTACK BLOCKER

Network Attack Blocker scans inbound traffic for activity typical of network attacks. Once an attempt to attack your computer is detected, Kaspersky Small Office Security blocks any network activity of the computer making an attack towards your computer.

By default, the blocking persists for one hour. You can edit the blockage settings (see page 132). A warning will appear on the screen stating that an attempted network attack has taken place, with specific information about the computer which attacked you. Descriptions of currently known network attacks (see section "Types of detected network attacks" on page 131) and methods to fight them, are provided in Kaspersky Small Office Security databases. The list of attacks which the Network Attack Blocker can detect is updated when the application's databases are updated (see section "Update" on page 72).

IN THIS SECTION:

Types of detected network attacks 131

Enabling and disabling Network Attack Blocker 132

Editing the blockage settings 132

TYPES OF DETECTED NETWORK ATTACKS

Nowadays, a great number of network attacks exist. These attacks exploit vulnerabilities of the operating system and other software, system-type or otherwise, installed on your computer.

To ensure the security of your computer, you must know what kinds of network attacks you might encounter. Known network attacks can be divided into three major groups:

- *Port scan* – this threat type is not an attack itself but it usually precedes one, since it is one of the common ways of obtaining information about a remote computer. The UDP / TCP ports used by the network tools on the computer targeted by an intruder are scanned to find out their status (closed or open).

  Port scans can tell a hacker what types of attacks work on that system, and what types do not. In addition, the information obtained by the scan (a model of the system) helps the malefactor to know what operating system the remote computer uses. This, in turn, further restricts the number of potential attacks, and, correspondingly, the time spent perpetrating them. It also aids a hacker in attempting to use vulnerabilities characteristic of the operating system.

- *DoS attacks*, or Denial of Service attacks are attacks which cause an unstable performance of a system or its crash. Attacks of this type may affect the operability of information resources under attack (for example, blocking Internet access).

  There are two basic types of DoS attacks:

  - sending the target computer specially created packets that the computer does not expect, which cause the system either to restart or to stop;

  - sending the target computer many packets within a timeframe that the computer cannot process, which causes system resources to be exhausted.

  The most flagrant examples for this group of attacks are the following types:

  - The *Ping of death* attack consists of sending an ICMP packet with a size greater than the maximum of 64 KB. This attack can crash some operating systems.

  - *Land attack* consists of sending a request to an open port on the target computer to establish a connection with itself. This attack sends the computer into a cycle, which intensifies the load on the processor and can lead to the crashing of some operating systems.

  - The *ICMP Flood* attack consists of sending a large quantity of ICMP packets to your computer. The computer attempts to reply to each inbound packet, which slows the processor to a crawl.

  - The *SYN Flood* attack consists of sending a large quantity of queries to a remote computer to establish a fake connection. The system reserves certain resources for each of those connections, which completely drains your system resources, and the computer stops reacting to other connection attempts.

- *Intrusion attacks*, which aim to take over your computer. This is the most dangerous type of attack, because if it is successful, the hacker takes total control of your system.

  Hackers use this attack to obtain confidential information from a remote computer (for example, credit card numbers, passwords), or to penetrate the system to use its computing resources for malicious purposes later (e.g., to use the invaded system in a zombie network, or as a platform for new attacks).

  This group is the largest in number of attacks included. They may be divided into three groups depending on the operating system installed on the user's computer: Microsoft Windows attacks, Unix attacks, and the common group for network services available in both operating systems.

  The following types of attacks are the most common among those using the network resources of operating systems:

  - *Buffer overflow attacks*. Buffer overflow may be caused by lack (or insufficiency) of control when working with data arrays. This is one of the oldest vulnerability types and the easiest for hackers to exploit.

  - *Format string attacks*. Format string errors arise from insufficient control of input values for I/O functions, such as *printf()*, *fprintf()*, *scanf()*, and others, from the standard C library. If an application has this vulnerability, the hacker is able to send queries created with a special technique and can take total control of the system.

    Intrusion Detection System automatically analyzes and prevents attempts to exploit these vulnerabilities in the most common network services (FTP, POP3, IMAP) if they are running on the user's computer.

  - *Attacks aimed at computers with Microsoft Windows* are based on the use of vulnerabilities of the software installed on a computer (such as Microsoft SQL Server, Microsoft Internet Explorer, Messenger, and system components available via the network – DCom, SMB, Wins, LSASS, IIS5).

  In addition, the use of various malicious scripts, including scripts processed by Microsoft Internet Explorer and Helkern-type worms, can be classified as isolated incidents of intrusion attacks. The essence of this attack type consists of sending a special type of UDP packets to a remote computer that can execute malicious code.

ENABLING AND DISABLING NETWORK ATTACK BLOCKER

By default, Network Attack Blocker is enabled, functioning in optimum mode. You can disable Network Attack Blocker, if necessary.

To enable or disable the Network Attack Blocker:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Network Attack Blocker** component.
4. In the right part of the window, uncheck the **Enable Network Attack Blocker** box if you need to disable this component. Check this box if you need to enable the component.

EDITING THE BLOCKAGE SETTINGS

By default, Network Attack Blocker blocks the activity of a computer making an attack for one hour. You can cancel blockage of the selected computer or change the time of blockage.

To modify the time for which the computer making an attack will be blocked:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Network Attack Blocker** component.
4. In the right part of the window, check the **Add the attacking computer to the list of blocked computers for** box and specify the time of blockage.

To unblock the computer making an attack:

1. Open the main application window.
2. In the left part of the window, select the **Protection Center** section.
3. In the right part of the window, in the **Online activity** section, click the **Network Monitor** link to open the **Network Monitor** window.
4. Select the blocked computer on the **Blocked computers** tab and unlock it using the **Unblock** link.

ENCRYPTED CONNECTIONS SCAN

Connecting using the SSL/TLS protocols protects data exchange channel on the Internet. The SSL/TLS protocols allows identifying the parties exchanging data using electronic certificates, encoding the data being transferred, and ensuring their integrity during the transfer.

These features of the protocol are used by hackers to spread malicious programs, since most antivirus applications do not scan SSL/TLS traffic.

Kaspersky Small Office Security scans encrypted connections using a Kaspersky Lab's certificate.

If an invalid certificate is detected when connecting to the server (for example, if the certificate is replaced by an intruder), a notification will pop up containing a suggestion to either accept or reject the certificate.

If you are sure that connection with a website is always secure, in spite of an invalid certificate, you can add the website into the list of trusted URLs. Kaspersky Small Office Security will no longer scan the encrypted connection with this website.

To enable encrypted connections scan, please do the following:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Network** subsection.
4. In the right part of the window, check the **Scan encrypted connections** box and click the **Install certificate** button.
5. In the window that opens, click the **Install Certificate** button. This will start a wizard with instructions to follow for a successful installation of the certificate.

The automatic installation of the certificate will only be available in Microsoft Internet Explorer. To scan encrypted connections in Mozilla Firefox or Opera, you should install the Kaspersky Lab's certificate manually.

SCANNING ENCRYPTED CONNECTIONS IN MOZILLA FIREFOX

Mozilla Firefox browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Firefox, you should install the Kaspersky Lab's certificate manually.

To install theKaspersky Lab certificate:

1. In the browser menu, select the **Tools** → **Settings** item.
2. In the window that opens, select the **Additional** section.
3. In the **Certificates** section, select the **Security** tab and click the **View Certificates** button.
4. In the window that opens, select the **Authorities** tab and click the **Restore** button.
5. In the window that opens, select the Kaspersky Lab certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. In the window that opens, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

To install thecertificate for Mozilla Firefox version 3.x:

1. In the browser menu, select the **Tools** → **Settings** item.
2. In the window that opens, select the **Additional** section.
3. On the **Encryption** tab, click the **View Certificates** button.
4. In the window that opens, select the **Authorities** tab and click the **Import** button.
5. In the window that opens, select the Kaspersky Lab certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. In the window that opens, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

If your computer runs under Microsoft Windows Vista, the path to the Kaspersky Lab's certificate file will be as follows: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

SCANNING ENCRYPTED CONNECTIONS IN OPERA

Opera browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Opera, you should install Kaspersky Lab's certificate manually.

To install theKaspersky Lab certificate:

1. In the browser menu, select the **Tools** → **Settings** item.
2. In the window that opens, select the **Additional** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that opens, select the **Vendors** tab and click the **Import** button.
5. In the window that opens, select the Kaspersky Lab certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. In the window that opens, click the **Install** button. Kaspersky Lab's certificate is installed. To view information about the certificate, and to select actions for which the certificate will be used, select the certificate in the list and click the **View** button.

To install theKaspersky Lab's certificate for Opera version 9.x:

1. In the browser menu, select the **Tools** → **Settings** item.
2. In the window that opens, select the **Additional** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that opens, select the **Authorities** tab and click the **Import** button.
5. In the window that opens, select the Kaspersky Lab certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. In the window that opens, click the **Install** button. Kaspersky Lab's certificate is installed.

If your computer runs under Microsoft Windows Vista, the path to the Kaspersky Lab's certificate file will be as follows: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

NETWORK MONITOR

Network Monitor is a tool used to view information about network activities in real time.

To start Network Monitor:

1. Open the main application window.
2. In the left part of the window, select the **Protection Center** section.
3. Click the **Network Monitor** link to open the **Network Monitor** window, where information about network activity is displayed.

CONFIGURING THE PROXY SERVER

If the computer's Internet connection is established via a proxy server, you may need to edit its connection settings. Kaspersky Small Office Security uses these settings for certain protection components, as well as for updating the databases and application modules.

If your network includes a proxy server using a non-standard port, you should add the port number to the list of monitored ports (see section "Creating a list of monitored ports" on page 135).

To configure the proxy server:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Proxy server** subsection.
4. Check the **Use proxy server** box and configure connection to the proxy server.

CREATING A LIST OF MONITORED PORTS

Such protection components as Mail Anti-Virus, Anti-Spam, Web Anti-Virus and IM Anti-Virus monitor the data streams transferred via specific protocols and passing certain open TCP-ports on your computer. For example, Mail Anti-Virus scans information transferred via SMTP, while Web Anti-Virus scans information transferred via HTTP, HTTPS, and FTP.

You can enable monitoring all or just the selected network ports. If you configure the product to monitor the selected ports, you can specify the list of applications, for which all ports will be monitored. We recommend that you expand this list by including applications that receive or transfer data via FTP.

To add a port to the list of monitored ports:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Network** subsection.
4. Click the **Select** button in the right part of the window.

   The **Network ports** window opens.
5. Click the **Add** link located under the list of ports in the top part of the window to open the **Network port** window, and enter the number and description of a port.

To exclude a port from the list of monitored ports:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Network** subsection.
4. Click the **Select** button in the right part of the window.

   The **Network ports** window opens.
5. In the list of ports in the top part of the window, uncheck the box next to the description of the port that should be excluded.

To create the list of applications for which you wish to monitor all ports:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Network** subsection.
4. Click the **Select** button in the right part of the window.

   The **Network ports** window opens.
5. Check the **Monitor all ports for specified applications** box and in the list of applications below check the boxes for the names of the applications for which all ports should be monitored.
6. If an application is not included in the list, add it as follows:

   a. To select a method for adding an application into the list, open the menu by clicking the **Add** link located under the list of applications, and select an item from the menu:

   - Select **Browse** to specify the location of the executable file. After you have selected the executable file, the **Application** window opens.
   - Select **Applications** to select an application from the list of currently active applications. After selecting the application, the **Application** window will open.
7. In the **Application** window, enter the description for the application selected.

TRUSTED ZONE

Trusted zone is the user-created list of objects which should not be controlled by the application. In other words, it is a set of exclusions from the scope of Kaspersky Small Office Security protection.

Trusted zone is created based on the list of trusted applications (see section "Creating a list of trusted applications" on page 137) and exclusion rules (see section "Creating the exclusion rules" on page 138), with regard for the features of the objects being processed and the applications installed on the computer. Including objects into the trusted zone may be required if, for example, Kaspersky Small Office Security blocks access to an object or application although you are assured that this object / application is absolutely harmless.

For example, if you think objects being used by Microsoft Windows Notepad to be harmless and require no scan, thus trusting this application, add Notepad into the list of trusted applications to exclude scan of objects being used by this process.

Some actions classified as dangerous may be stated as safe by a number of applications. Thus, applications that automatically toggle keyboard layouts, such as Punto Switcher, regularly intercept text being entered on your keyboard. To take into account the specifics of such applications and disable the monitoring of their activity, you are advised to add them to the list of trusted applications.

When an application is added into the list of trusted ones, its file and network activities (including suspicious ones) become uncontrolled. So do its attempts to access the system registry. At the same time, the executable file and the trusted application's process is scanned for viruses as they were before. To completely exclude an application from the scan, you should use exclusion rules.

Excluding trusted applications from the scan allows to avoid problems of the application's compatibility with other programs (e.g. the problems of double scanning of network traffic of a third-party computer by Kaspersky Small Office Security and by another anti-virus application), as well as increase the computer's performance rate which is critical when using server applications.

In its turn, exclusion rules of trusted zone ensure the option to work with legal applications the may be used by intruders to do harm to the user's computer or data. These applications have no malicious features, but they may be used as auxiliary components of a malicious program. This category includes remote administration applications, IRC clients, FTP servers, various utility tools for halting or concealing processes, keyloggers, password hacking programs, dialers, and others. Such applications may be blocked by Kaspersky Small Office Security. To avoid blockage, you can configure exclusion rules.

Exclusion rule – is a set of conditions which determine that an object should not be scanned by Kaspersky Small Office Security. In any other case, the object is scanned by all protection components according to their respective protection settings.

Exclusion rules of the trusted zone may be used by several application components, such as File Anti-Virus (see section "File Anti-Virus" on page 77), Mail Anti-Virus, Web Anti-Virus, or when running virus scan tasks.

IN THIS SECTION:

Creating a list of trusted applications 137

Creating the exclusion rules 138

CREATING A LIST OF TRUSTED APPLICATIONS

By default, Kaspersky Small Office Security scans objects being opened, run, or saved by any program process, and monitors the activity of all applications and the network traffic they create. When you add an application to the list of trusted ones, Kaspersky Small Office Security excludes it from scan.

To add an application to the trusted list:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Threats and Exclusions** subsection.
4. In the right part of the window, in the **Exclusions** section click the **Settings** button.
5. In the window that opens, on the **Trusted applications** tab, click the **Add** link to open the application selection menu, and choose one of the following options:
   - Select **Browse** to specify the location of the executable file. After selecting the executable file, the **Exclusions for application** window will open.
   - Select **Applications** to select an application from the list of currently active applications. After selecting the application, the **Exclusions for application** window will open.
6. In the **Exclusions for applications** window that opens, check the boxes for the types of application's activity that should be excluded from scan.

You can change the scan settings for an application or delete it from the list by using the corresponding links at the bottom of the list. To remove an application from the list without its actual deletion, uncheck the box next to its name.

CREATING THE EXCLUSION RULES

If you use applications recognized by Kaspersky Small Office Security as legal ones that may be used by intruders to do harm to the user's computer or data, we recommend that you configure exclusion rules for them.

To create an exclusion rule:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Threats and Exclusions** subsection.
4. In the right part of the window, in the **Exclusions** section click the **Settings** button.
5. Click the **Add** link on the **Exclusion rules** tab in the window that opens.
6. In the **Exclusion rule** window that opens, edit the exclusion rule settings.

SAFE MODE OF APPLICATIONS EXECUTION

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Virtualization is a secure environment isolated from the main operating system and designed for running applications whose safety raises doubts.

When you use Safe Run, the real objects of the operating system do not undergo changes. So even if you run an infected application in Safe Run, all of its actions will be limited to the virtual environment without affecting the operating system.

Running Internet browsers in a safe environment ensures security when viewing web resources, including the protection against malware penetrating the computer and the protection of user data against any unauthorized attempts of changing

and deleting, as well as the possibility of deleting all objects accumulated during the Internet session: temporary files, cookies, history of web pages browsed, etc. Microsoft Internet Explorer is included in the list of applications running in safe mode, by default.

Running an application (see section "Running an application in safe mode" on page 139) in safe mode is performed depending on the mode selected. The option of creating shortcuts is provided for a quick start of applications in safe mode.

For the files saved or modified in safe mode to be available when working in standard mode, you should use the Safe Run Shared Folder created exclusively for those files and available both in safe mode and in standard mode. When clearing safe mode data, the files stored in this folder will not be deleted.

Safe mode of applications execution is completely unavailable on computers running Microsoft Windows XP x64.

The functionality of certain applications launched on computers running Microsoft Windows Vista x64 and Microsoft Windows 7 x64 is limited when operating in the safe environment. If such applications are started, the corresponding message will be displayed on the screen if you have configured the notifications (see page 222) about the **Application functionality is limited in safe mode** event.

IN THIS SECTION:

Running an application in safe mode 139

Creating the list of applications to run in safe mode 140

Creating a shortcut for program execution 141

Clearing Safe Run data 141

Using a shared folder 142

RUNNING AN APPLICATION IN SAFE MODE

If the **Always run in safe mode** option is not enabled for the application, it can be run in safe mode using one of the following ways:

- from the Microsoft Windows context menu;
- from the **Kaspersky Small Office Security main window** (see page 31);
- using existing shortcut (see section "Creating a shortcut for program execution" on page 141).

If the **Always run in safe mode** option is selected for the application, it will be launched in safe mode regardless of the run mode.

Applications running in safe mode, are highlighted with a green frame around the application window, and highlighted with green color in the list of applications monitored by Security Zone.

You are advised to use Microsoft Windows standard mode to install the applications with which you wish to work in safe mode in the future.

To run an application in safe mode from the Microsoft Windows context menu, please do the following:

1. Right-click to open the context menu for the selected object (shortcut or executable file of the application).
2. In the menu that opens, select the **Safe Run** item.

To run an application in safe mode from the Kaspersky Small Office Security main window, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. In the bottom part of the window, in the **Safe Run** section, open the context menu for the required application and select **Run**.

To run an application in safe mode using a shortcut, please do the following:

1. Open the folder in which a shortcut was created.
2. Run the application by double-clicking its shortcut.

CREATING THE LIST OF APPLICATIONS TO RUN IN SAFE MODE

In the Kaspersky Small Office Security main window, you can create the list of applications to run in safe mode. The list is displayed in the **Security Zone** section.

If you add to the list an application that allows working with several copies of it at the same time (such as Windows Internet Explorer), each new copy of it runs in safe mode after the application is added to the list. If you add to the list an application that allows using only one copy of it, that application must be restarted after it is added to the list.

When adding an application in the list of applications running in safe mode, you can enable the **Always run in safe mode** option for it. This means that the application will be run in safe mode regardless of the run mode, whether using Microsoft Windows standard tools, or Kaspersky Small Office Security tools.

You are not advised to enable the **Always run in safe mode** option for system applications and utilities, since this can lead to an improper functioning of the operating system.

To add an application to the list of applications running in safe mode, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. In the bottom part of the window, in the **Safe Run** section, open the menu by clicking the **Add** link.
4. In the menu that opens, select the necessary application. Once you select the **Browse** item, a window will open in which you should specify the path to an executable file. Once you select the **Applications** item, the list of applications currently running will open. After that, the application icon will be added to the list.

   To delete an application from the list of applications running in safe mode, select it in the list and click the **Delete** link.

To run an application in safe mode only, regardless of the run mode, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. In the bottom part of the window, in the **Safe Run** section, open the context menu for the required application and select the **Always run in safe mode** item.

   The ✓ box will be displayed next to the menu item.

CREATING A SHORTCUT FOR PROGRAM EXECUTION

To run applications quickly in safe mode, Kaspersky Small Office Security provides the possibility of creating shortcuts. This allows running the required application in safe mode, without opening the main application window or the Microsoft Windows context menu.

To create a shortcut to run an application in safe mode, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. In the bottom part of the window, in the **Safe Run** section, open the context menu for the required application and select the **Create shortcut** item.
4. Specify the path for saving a shortcut and its name in the window that opens. By default, a shortcut will be created in the *My Computer* folder of the current user, and it will be assigned the name corresponding to the application's process.

CLEARING SAFE RUN DATA

If an application runs in safe mode, all modifications performed by the application are performed within the scope of safe mode only. By default, at the next application startup, all changes made and files saved will be available during the safe mode session.

If you do not need the safe mode data any more, or if you need to restore the current settings for all applications running in Microsoft Windows standard mode, you can clear safe mode data.

If you do not want the changes you have made to be available for an application at the next run in safe mode, you can enable the **Clear Safe Run data on exit** mode for it. This means that the changes you have made during the session, will be automatically deleted after the application is closed.

Before clearing the data, saved in the safe mode, you should make sure that all information you may need for further work has been saved in the shared folder. Otherwise, the data is deleted without any possibility to restore them.

To clear Safe Run data:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. In the bottom part of the window, in the **Safe Run** section, click the **Clear** link.
4. In the window that opens, confirm data clearing.

To clear Safe Run data every time the application closes, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. In the bottom part of the window, in the **Safe Run** section, open the context menu for the required application and select the **Clear Safe Run data on exit** item.

   The ✓ box will be displayed next to the menu item and the sign will appear on the application icon in the list of applications running in safe mode.

   To cancel the clearing of safe mode data after the application is closed, select this box again.

USING A SHARED FOLDER

When working in safe mode, all changes required due to the application's operation, are only made in safe mode, so they do not affect the standard mode. Thus, files saved in safe mode cannot be transferred to the standard mode.

For the files saved or modified in safe mode to be available in standard mode, *Safe Run Shared Folder* can be used, provided by Kaspersky Small Office Security. All files saved in this folder when working in safe mode, will be available in standard mode.

The shared folder is a folder on a hard disk created at the Kaspersky Small Office Security installation.

The shared folder is created in the *%AllUsersProfile%\Application Data\Kaspersky Lab\SandboxShared* folder during application installation, and its location cannot be changed.

The shared folder is indicated with the icon in the Microsoft Windows Explorer. You can also go to the folder from the Kaspersky Small Office Security main window.

To open the shared folder from the Kaspersky Small Office Security's main window:

1. Open the main application window.
2. In the left part of the window, select the **Security Zone** section.
3. In the bottom part of the window, in the **Safe Run** section, click the **Shared Folder** link. The folder will open in a standard Microsoft Windows Explorer window.

QUARANTINE AND BACKUP

Quarantine is a special repository that stores the objects possibly infected with viruses. *Potentially infected objects* are objects suspected of being infected with viruses or their modifications.

A potentially infected object can be detected and quarantined by File Anti-Virus, Mail Anti-Virus, Proactive Defense or in the course of a virus scan.

Objects are quarantined in the following cases:

- Object code resembles a known but partially modified threat, or has malware-like structure but is not registered in the database. In this case objects are moved to Quarantine after heuristic analysis performed by the File Anti-Virus, Mail Anti-Virus or during anti-virus scan. Heuristic analysis rarely causes false alarms.
- The sequence of operations performed by an object looks suspicious. In this case objects are moved to Quarantine after the analysis of their behavior by Proactive Defense component.

When you place an object in Quarantine, it is moved, not copied: the object is deleted from the disk or email, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

Backup storage is designed for storing backup copies of infected objects that could not been disinfected immediately after detection.

It is possible that after the next databases update, Kaspersky Small Office Security will be able to identify the threat unambiguously and neutralize it. Due to this fact, the application scans quarantine objects after each update (see page 76).

IN THIS SECTION:

Storing quarantine and backup objects 143

Working with quarantined objects 143

STORING QUARANTINE AND BACKUP OBJECTS

The default maximum storage duration for objects is 30 days. Then the objects will be deleted. You can cancel the time-based restriction or change the maximum objects storage duration.

Additionally, you can specify maximum size of Quarantine and Backup. If the maximum size value is reached, the content of Quarantine and Backup is changed with new objects. By default, the maximum size restriction is disabled.

To modify the object maximum storage time:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Reports and Storages** subsection.
4. In the right part of the window, check the **Store objects no longer than** box and specify maximum storage duration for quarantined objects.

To configure the maximum Quarantine and Backup size:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Reports and Storages** subsection.
4. In the right part of the window, check the **Maximum size** box and specify the maximum Quarantine and Backup size.

WORKING WITH QUARANTINED OBJECTS

The quarantine of Kaspersky Small Office Security lets you perform the following operations:

- quarantine the files that you suspect of being infected;
- scan and disinfect all potentially infected quarantine objects using the current database of Kaspersky Small Office Security;
- restore files to a specified folder to source folders from which they were moved to quarantine (by default);
- delete any quarantined object or group of objects;
- send quarantined objects to Kaspersky Lab for analysis.

You can move an object to Quarantine using one of the two methods:

- using the **Move to Quarantine** link in the **Protection state** window;
- using the context menu of the object.

- *To move an object to Quarantine from the **Protection state** window:*

  1. Open the main application window.
  2. In the top part of the window, use the **Quarantine** link to open the **Protection status** window.
  3. On the **Detected threats** tab, follow the **Quarantine** link.
  4. In the window that opens, select the object that you want to move to Quarantine.

- *To move an object to Quarantine using the context menu:*

  1. Open Microsoft Windows Explorer and go to the folder that contains the object that you want to move to Quarantine.
  2. Right-click to open the context menu of the object and select **Move to Quarantine**.

- *To scan a quarantined object:*

  1. Open the main application window.
  2. In the top part of the window, use the **Quarantine** link to open the **Protection status** window.
  3. On the **Detected threats** tab, select the object that needs to be scanned.
  4. Right-click to open the context menu and select **Scan**.

- *To disinfect all quarantined objects:*

  1. Open the main application window.
  2. In the top part of the window, use the **Quarantine** link to open the **Protection status** window.
  3. On the **Detected threats** tab, click the **Disinfect all** link.

- *To restore a quarantined object:*

  1. Open the main application window.
  2. In the top part of the window, use the **Quarantine** link to open the **Protection status** window.
  3. On the **Detected threats** tab, select the object that needs to be restored.
  4. Right click to open the object's context menu and select **Restore**.

- *To remove quarantined objects:*

  1. Open the main application window.
  2. In the top part of the window, use the **Quarantine** link to open the **Protection status** window.
  3. On the **Detected threats** tab, select the object that needs to be deleted.
  4. Right-click the object to open the context menu and select **Delete from the list**.

To send a quarantined object toKaspersky Lab for analysis:

1. Open the main application window.
2. In the top part of the window, use the **Quarantine** link to open the **Protection status** window.
3. On the **Detected threats** tab select the object that needs to be sent for analysis.
4. Right-click to open the context menu and select **Send**.

BACKUP

During the backup process, backup copies of the chosen files are created in a special storage area.

Backup storage is a specially assigned area of disk space or a data storage media. Storages are used by the backup tasks for storing backup copies of data.

When creating a storage area (see section "Creating a backup storage area" on page 146), the user selects the data medium, specifies the name of the new storage area and the settings for storing backup copies. Also, stored data may be password-protected against unauthorized access. After that, service information about the storage area is recorded onto the data medium.

To carry out data backup, backup tasks are created (see section "Creating a backup task" on page 148). *Backup task* is a user-defined collection of parameters that determines the selection of data subject to backup, storage area for backup copies, and backup conditions. Tasks are restartable (manually or by schedule).

Backup copies of files created within the framework of a single task are stored in *archives*. Archives of backup copies are placed into a storage after having been assigned the name matching that of the task.

To restore data from backup copies, run the restoring procedure (see section "Restoring data" on page 149), or use the Kaspersky Restore Utility. Files may be restored from backup copies either into their initial location, or into any available folder.

All events related to backup are recorded in the report (see section "Viewing event report" on page 151).

IN THIS SECTION:

Creating a backup storage area 146

Connecting an existing storage 146

Clearing a storage 147

Removing a storage 147

Creating a backup task 148

Running a backup task 148

Restoring data 149

Searching for backup copies 150

Viewing backup copy data 151

Viewing event report 151

CREATING A BACKUP STORAGE AREA

A backup storage area may be created using the wizard. Backup Storage Creation Wizard may be launched using one of the two following modes:

- from the main module window;
- from the Backup Task Creation Wizard (see section "Creating a backup task" on page 148).

This wizard consists of a series of screens (or steps) navigated using the **Back** and the **Next** buttons. To close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing links in the top part of the window.

To create a backup storage area, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Storage** section and click the **Create** button.
5. Backup Storage Creation Wizard will be launched. Let us take a closer look at the wizard's steps:
   a. In the left part of the **Drive** window, select the type of data storage medium which will be used as a backup storage.

      To ensure data security, we recommend that you create backup storages on removable disk drives.

   b. In the **Protection** window, set a password to protect data against unauthorized access (if necessary).
   c. In the **File versions** window, set a limit on the number of file versions which may coexist within the storage, and specify the time interval for storing file versions (if necessary).
   d. In the **Summary** window, enter the name for the new storage and confirm the storage creation with the settings you have specified.

CONNECTING AN EXISTING STORAGE

If you have created a storage with Kaspersky Small Office Security but it is unavailable on the computer you are currently using (for example, after the operating system is reinstalled, or if the storage is copied from another computer), you will need to connect that storage in order to start working with the data.

To connect an existing storage, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.

4. In the window that opens, select the **Storage** section and click the **Connect** button.
5. Select a storage type and specify the required connection settings in the **Connect storage** window.

   If the settings are specified properly, the storage appears on the list.

CLEARING A STORAGE

If storage volume is not sufficient for your current operations, you can delete obsolete versions and backup copies of files which have been already deleted from the computer.

To clear a storage, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Storage** section.
5. Select the storage you wish to clear and click the **Clear** button.
6. In the **Clear storage** window that opens, select the file versions that should be deleted from the storage.

REMOVING A STORAGE

To remove a storage for backup data, you should use Storage Removal Wizard. During the removal, you are asked to determine actions to be performed on the data in the storage, that is to be removed, and on the tasks, that use the storage for backup copying.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing buttons in the top part of the window.

To remove a backup storage, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Storage** section.
5. Select the storage you wish to delete and click the **Delete** button.
6. Backup Storage Removal Wizard will be launched. Let us take a closer look at the wizard's steps:

   a. Select an action to perform on the backup copies that are located within the storage to be removed, in the **Content** window.

   b. Select an action to perform with the tasks that use the storage for backup copy, in the **Tasks** window.

   c. Confirm the removal of the storage with selected settings in the **Summary** window.

CREATING A BACKUP TASK

Backup tasks are used for creating backup copies of files and are a set of the following settings:

- a set of files for which backup copies will be created;
- a storage in which backup copies of files will be created;
- conditions of backup process startup.

A backup task may be created using the wizard.

This wizard consists of a series of screens (or steps) navigated using the **Back** and the **Next** buttons. To close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing buttons in the top part of the window.

To create a backup task, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Backup** section and click the **Create** button.
5. The Backup Task Creation Wizard will be launched. Let us take a closer look at the wizard's steps:
   a. In the **Content** window, select the objects for which backup copies will be created.
   b. In the **Storage** window, select the storage in which backup copies of files will be created.
   c. In the **Schedule** window, specify the conditions for running the task.
   d. In the **Summary** window, enter the name for the new task and confirm the task creation with the settings you have specified.

RUNNING A BACKUP TASK

Backup tasks may be run automatically (by a schedule) or manually. The actual task run mode is displayed in the list of tasks (see the figure below).

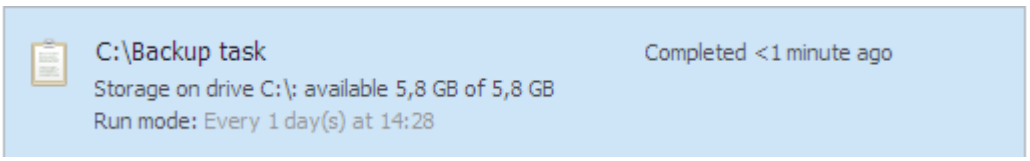

Figure 9. Information about the backup task

Automatic run schedule is configured at the creation of a task; however, it may be subsequently changed.

If required, you can start any task manually.

To run a backup task manually, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Backup** section.
5. From the list in the right part of the window, select the task which should be executed, and click the **Run** link.

The line of the task you have selected displays the time elapsed since the beginning of the task run. Task run may be paused or cancelled by using respective buttons in the top part of the window.

Task execution results in creating an archive of current backup copies in the storage.

RESTORING DATA

The data may be restored from the backup copies of files, if necessary. Backup procedure is only available for connected storages. Being restored, data from backup copies are saved into the folder you have selected.

Files may be restored in various ways:

- restore the most recent file version;
- select a version to restore by date.

To restore the most recent file version, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Restore** section.
5. Select the storage where the required backup copies are located and click the **Restore** button.
6. In the top part of the **Restoring files from storage** window, in the **Backup set** dropdown list, select the name of the task which has resulted in creating an archive with the required backup copies, when executed.
7. Select the files that need to be restored. To do this, check the boxes next to the required files in the list. To select all files, click the **Select all** button in the bottom part of the list. Click the **Restore** button in the top part of the window.
8. In the **Restore** window that opens, select the location to save restored files and the condition of saving if files' names coincide. Click the **Restore** button.

To select the required file version, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Backup and Restore** button.
4. In the window that opens, select the **Restore** section.
5. Select the storage where the required backup copies are located and click the **Restore data** button.
6. In the top part of the **Restoring files from storage** window, in the **Backup set** dropdown list, select the name of the task which has resulted in creating an archive with the required backup copies, when executed.

7. Select the file whose version you want to specify. To do so, check the box next to the file you need. Click the **Versions** button in the top part of the window.

8. In the **File versions** window that opens, select the date of the version you need to restore, and click the **Restore** button.

9. In the **Restore** window that opens, select the location to save restored files and the condition of saving if files' names coincide. Click the **Restore** button.

SEARCHING FOR BACKUP COPIES

To search for backup copies in a storage, you can use the filter and the search field.

Backup copy filter allows displaying only the copies which conform to the search criteria you have specified.

You can find a backup copy in the archive, by entering its name in the search field.

To display the backup copies of files which have not been included into the list of files subject to backup at the last execution of the task (e.g., which have been deleted from the computer), check the **Show deleted files** box.

To filter backup copies, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Backup and Restore** button.

4. In the window that opens, select the **Restore** section.

5. In the right part of the window, select a storage and click the **Restore** button.

6. In the top part of the **Restoring files from storage** window, select the search criteria in the filter:

   - In the **Backup set** dropdown list, select the name of the task which has resulted in creating an archive with the required backup copies, when executed.

   - In the **Date** dropdown list, select the date when the archive with the required backup copies was created.

   - From the **Category** dropdown list, select the file types for which backup copies should be found.

   As a result, the list will only contain backup copies that meet the specified conditions.

To find a backup copy by its name, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Backup and Restore** button.

4. In the window that opens, select the **Restore** section.

5. In the right part of the window, select a storage and click the **Restore** button.

6. In the top part of the **Restoring files from storage** window, in the **Search** field, enter the full name of a file or a part of it.

As a result, the list will only contain the backup copies of files whose names start with the characters entered.

VIEWING BACKUP COPY DATA

Before restoring data, you can view the contents of the selected version of backup copy. To do so, you can open the latest version or select a version based on the date specified.

- *To open the most recent file version, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Backup and Restore** button.

4. In the window that opens, select the **Restore** section.

5. Select the storage where the required backup copies are located and click the **Restore** button.

6. In the top part of the **Restoring files from storage** window, in the **Backup set** dropdown list, select the name of the task which has resulted in creating an archive with the required backup copies, when executed.

7. In the right part of the window, select the required file from the list and click the **Open** button.

- *To open a file version based on the specified date, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Backup and Restore** button.

4. In the window that opens, select the **Restore** section.

5. Select the storage where the required backup copies are located and click the **Restore** button.

6. In the top part of the **Restoring files from storage** window, in the **Backup set** dropdown list, select the name of the task which has resulted in creating an archive with the required backup copies, when executed.

7. In the right part of the window, select the required file from the list and click the **Versions** button.

8. In the **File versions** window that opens, select the required date and click the **Open** button.

VIEWING EVENT REPORT

Each event related to data backup and restore is displayed in the report.

- *To get a backup module report, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Backup and Restore** button.

4. In the window that opens, click the **Report** link in the top part of the window.

5. In the **Report** window that opens, specify the event display settings.

WEB POLICY MANAGEMENT

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Web Policy Management allows the control of actions of users taken on the computer and on the network. The concept of control provides the option to restrict access to resources and applications as well as view reports of users' activities. This allows the employer to ensure compliance with the company's rules and regulations regarding the use of the computer and the Internet, and prevent any potential damage that might result from a violation of these rules and regulations.

Web Policy Management allows you to reduce risks posed by the computer and the Internet. To do this, the following module's functions are used:

- limiting the time of computer and Internet use;
- creating lists of allowed and blocked applications as well as temporarily limiting number of startups for allowed applications;
- creating lists of allowed and blocked websites, specifying categories of websites with content not recommended for viewing;
- enabling the safe search mode involving search engines (links to websites with suspicious content are not displayed in the search results);
- restricting file downloads from the Internet;
- creating lists of contacts which are allowed or blocked for communication via IM clients and social networks;
- viewing message logs from IM clients and social networks;
- blocking sending of specified privacy data;
- searching for specified key words in message logs.

All these restrictions can be enabled independently from each other, which allows you to flexibly configure Web Policy Management for various users. For each account, you can view reports which contain events for the categories being controlled that the component has logged over the specified period.

To start managing the component, you should enter the Administrator password (see section "How to restrict access to Kaspersky Small Office Security settings" on page 56). If you have not yet set a password for managing Kaspersky Small Office Security, you will be offered to do this.

IN THIS SECTION:

Configure Web Policy Management for the user 153

Viewing reports of user's activity 161

CONFIGURE WEB POLICY MANAGEMENT FOR THE USER

You can enable and configure Web Policy Management for each account separately, by imposing different limits on different users. You can also disable Web Policy Management for the users whose activity needs no control.

You need to perform the authentication procedure to begin managing the component. After you have entered the administrator password, you can enable, pause or disable Web Policy Management, and also modify its settings.

IN THIS SECTION:

Enabling and disabling Web Policy Management 153

Saving and downloading Web Policy Management settings 154

Displaying an account in Kaspersky Small Office Security 155

Time of computer use 155

Running applications 156

Time of Internet use 156

Viewing websites 156

Downloading files from the Internet 157

Safe search mode 157

Communicating via IM clients 158

Communicating via social networks 159

Sending confidential information 160

Searching for key words 160

ENABLING AND DISABLING WEB POLICY MANAGEMENT

You can enable and disable Web Policy Management individually for every account. E.g., there is no need to control the activity of the user of the administrator account – Web Policy Management for this can be disabled. For other users whose activity should be controlled, the Web Policy Management should be enabled and configured, for example, by loading the standard configuration from a template.

You can enable or disable Web Policy Management for the current account using the main window and the context menu of the application icon.

- *To enable Web Policy Management, please do the following:*

  1. Open the main application window.
  2. Select the **Web Policy Management** section in the left part of the window.
  3. Click the **Enable Web Policy Management** button in the right part of the window..

- *To pause Web Policy Management, please do the following:*

  1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. Click the **Pause Web Policy Management** button in the right part of the window.

4. In the **Pause Web Policy Management** window, select the mode of operation resuming.

You can also pause or resume Web Policy Management for the current user account from the context menu of the application icon (see page 30).

SAVING AND DOWNLOADING WEB POLICY MANAGEMENT SETTINGS

If you have configured Web Policy Management for an account, you can save the settings as a file. You can import the settings from this file for quick configuring in the future. Furthermore, you can apply the control settings defined for another account or a configuration template (predefined set of rules for different types of users).

After the import is completed, you can always modify the settings that you have selected for an individual account.

To save the control settings to a file, please do the following:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the user account whose control settings should be saved, and click the **Configure policies** button.

4. In the window that opens, click the **Export settings** link in the top part of the window and save the configuration file.

To load the control settings from file, perform the following steps:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the account for which the control settings should be loaded, and click the **Configure policies** button.

4. In the window that opens, click the **Import settings** link in the top part of the window.

5. Use the **Load control settings** window that opens to select the **File containing the previously exported settings** option and specify the file location.

To apply the settings of another account, perform the following steps:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the account for which the control settings should be applied, and click the **Configure policies** button.

4. In the window that opens, click the **Import settings** link in the top part of the window.

5. In the **Load control settings** window that opens, select the **Another user** option and specify the account whose settings you need to use.

To use a configuration template, perform the following steps:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the account for which predefined control settings should be used, and click the **Configure policies** button.

4. In the window that opens, click the **Import settings** link in the top part of the window.

5. In the **Load control settings** window that opens, select the **Template** option and specify the template, whose settings you need to use.

DISPLAYING AN ACCOUNT IN KASPERSKY SMALL OFFICE SECURITY

You can select an alias and an image with which your account should be displayed in Kaspersky Small Office Security.

To configure an alias and an image for an account, please do the following:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the account for which the display settings should be configured, and click the **Configure policies** button.

4. In the window that opens, in the **Additional** section, select the **Display** component. Enter an alias for the account and select an image to display.

TIME OF COMPUTER USE

You can set up a schedule of user's access to the computer (specifying days of week and time of day) and limit total time of computer use per 24 hours.

15 and 5 minutes before the expiration of allowed time of computer access, Kaspersky Small Office Security displays a warning message that the computer will be turned off. This allows to close the connection in a timely fashion and save the necessary data. Once the allowed time is expired, Kaspersky Small Office Security displays a notification that the schedule of computer access has been broken, and turns off the computer.

To limit the time of computer use:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.

4. In the window that opens, in the **Computer** section, select the **Usage** component.

5. In the **Control Computer Operating Time** window that opens, check the **Enable control** box and specify time restrictions.

RUNNING APPLICATIONS

You can allow or block the running of specified programs and impose time limits on startup.

To restrict applications and games launch:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.
4. In the window that opens, in the **Computer** section, select the **Running applications** component.
5. In the **Control Applications Usage** window that opens, check the **Enable control** box.
6. Create lists of applications allowed and blocked for running on the **Allowed** and **Blocked** tabs, and set the run schedule for allowed applications.

TIME OF INTERNET USE

You can restrict the time which the user spends in the Internet. To do this, you can set up a schedule of Internet use (specifying days of week and time of day when access should be granted or denied) and limit total time of Internet use per 24 hours.

Ten minutes before the expiration of allowed time of Internet use, Kaspersky Small Office Security displays a warning message that connection will be terminated. This allows to close the connection in a timely fashion and save the necessary data. Once the allowed time is expired, Kaspersky Small Office Security displays a notification that the schedule of Internet sessions has been broken, and terminates connection with the Internet.

To limit the time of Internet use:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.
4. In the window that opens, in the **Internet** section select the **Usage** component.
5. In the **Control using the Internet** window that opens, check the **Enable control** box and specify time restrictions.

VIEWING WEBSITES

You can set restrictions on certain web resources access depending on their content. To do this, you should create lists of allowed and blocked web pages, as well as choose the categories of web sites, access to which should be blocked.

To restrict the time of web resource access, do the following:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.
4. In the window that opens, in the **Internet** section, select the **Access to websites** component.

5. In the **Control access to websites** window that opens, check the **Enable control** box and impose the restrictions on access to web sites.

   On the **Blocked URLs** and **Allowed URLs** tabs, you can enter the addresses of allowed and blocked web sites. On the **Not recommended** tab, you can choose the categories of web sites, access to which should be blocked.

6. If you want to allow access to the listed web sites only, check the **Block websites not included into the "Allowed URLs" list** box.

   If you have checked the **Block websites not included into the "Allowed URLs" list** box, you need to add the address of the proxy server to the **Allowed URLs** list to connect to the Internet using a proxy server.

DOWNLOADING FILES FROM THE INTERNET

You can restrict file types that can be downloaded.

To restrict download of files from the Internet:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.
4. In the window that will open, in the **Internet** section select the **Downloading files** component.
5. In the **Control downloading files from the Internet** window that opens, check the **Enable control** box and select the file categories that should be allowed for download.

SAFE SEARCH MODE

Some search engines are designed to protect users against unsolicited content of web resources. To do this, when indexing websites, key words and phrases, resources' addresses and categories are analyzed. When the safe search mode is enabled, search results do not include websites related to unwanted categories, such as porn, drug abuse, or violence.

Web Policy Management allows to switch on the safe search mode for the Google and Bing search engines simultaneously.

To switch on the safe search mode, please do the following:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.

4. In the window that opens, in the **Internet** section, select the **Safe search** component.

5. In the **Control search results** window that opens, check the **Enable safe search mode** box.

COMMUNICATING VIA IM CLIENTS

Controlling instant messaging means controlling correspondence contents and contacts with which the messaging is allowed. You can create lists of allowed and blocked contacts, specify key words (see section "Key words search" on page 160) that all incoming messages will be checked for, and enter private data (see section "Sending confidential information" on page 160) that are prohibited to be sent.

If communication with a contact is blocked, all messages addressed to this contact or received from it will be filtered out. Information about blocked messages and key words encountered in them is displayed in a report. In the full report you can see messaging history for each contact.

The following restrictions are imposed on communication monitoring:

- If an IM client had been run before Web Policy Management has been enabled, communication monitoring will not start until the IM client is restarted.

- When using an HTTP proxy, communication is not monitored.

The current version of Web Policy Management monitors communication via the following IM clients:

- ICQ;
- QIP;
- Windows Live Messenger (MSN);
- Yahoo Messenger;
- GoogleTalk;
- mIRC;
- Mail.Ru Agent;
- Psi;
- Miranda;
- AOL Instant Messenger (AIM);
- Jabber.

Many IM clients use encrypted connection. To control messaging via such programs, you will need to enable the scan of encrypted connections (see page 133).

To restrict contacts available for communication via IM clients:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.

4. In the window that opens, in the **Messaging** section, select the **Instant messaging** component.

5. In the **Control Instant Messaging** window that opens, check the **Enable control** box.
6. On the **Allowed** and **Blocked** tabs, create lists of allowed and blocked contacts.
7. In the **Action** dropdown list, select the default action for contacts not included in your lists.

You can also allow or block communication with the contact you have selected from the report on events for that account.

To view the report:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. Click the **Report** button in the right part of the window.

   In the window that opens, in the **Messaging** section, select the **Instant messaging** component.

   The window displays a report on the user's instant messaging activity.

COMMUNICATING VIA SOCIAL NETWORKS

Controlling communication via social networks consists in controlling contacts allowed for communication and message logs. You can create lists of allowed and blocked contacts, specify key words (see section "Key words search" on page 160) that all incoming messages will be checked for, and enter private data (see section "Sending confidential information" on page 160) that are prohibited to be sent.

If communication with a contact is blocked, all messages addressed to this contact or received from it will be filtered out. Information about blocked messages and key words encountered in them is displayed in a report. In the full report you can see messaging history for each contact.

Some social networks, such as Twitter, use the encrypted connections. To scan the traffic generated by those networks, you should enable the scan of encrypted connections (see page 133).

The current version of Web Policy Management ensures control over instant messaging in the following social networks:

- Facebook;
- Twitter;
- MySpace.

To restrict contacts available for communication via social networks:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.
4. In the window that opens, in the **Messaging** section, select the **Social Networking** component.
5. In the **Control Social Networking** window that opens, check the **Enable control** box.
6. In the **Action** dropdown list, select the default action for contacts not included in your lists.

You can also allow or block communication with the contact you have selected from the detailed report on events for that account.

7. Close the configuration window and click the **Report** button.

8. In the window that opens, in the **Messaging** section, select the **Social Networking** component.

   In the right part of the window that opens, a list of contacts will appear, displaying the contacts from which a message has been received or to which a message has been sent.

9. Specify an action (block or allow messaging) for the selected contacts.

   The contacts will be automatically added into the list of controlled contacts, which can be viewed in the **Settings** window, in the **Social Networking** section.

SENDING CONFIDENTIAL INFORMATION

You can block sending data that contain confidential information via IM clients, social networks, and when sending data to websites. To do this, you should create a list of records that contain privacy data, such as physical address and phone number.

Attempts of sending listed data are blocked; information about blocked messages is displayed in a report.

To block sending of private data:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.

4. In the window that opens, in the **Messaging** section, select the **Private Data** component.

5. In the **Control Sending Private Data** window that opens, check the **Enable control** box. Add the record to the list of data forbidden to be sent by clicking the **Add** link.

SEARCHING FOR KEY WORDS

You can check user's messages for specified words and word combinations when communicating via IM clients, social networks, and when sending data to websites.

If some listed key words are detected in the messages, this is displayed in a report.

If you have disabled control of messaging via IM clients, social networks, or control of websites being visited, key words are not searched for.

To enable key words control in the messaging, please do the following:

1. Open the main application window.

2. Select the **Web Policy Management** section in the left part of the window.

3. In the right part of the window, select the user account on which a restriction should be imposed, and click the **Configure policies** button.

4. In the window that opens, in the **Messaging** section, select the **Key words** component.

5. In the **Control Word Usage** window that opens, check the **Enable control** box. Add the record to the list of key words that are controlled in messaging, by clicking the **Add** link.

VIEWING REPORTS OF USER'S ACTIVITY

For every user account under Web Policy Management, you can view a report on different categories of the controlled events.

To view the report:

1. Open the main application window.
2. Select the **Web Policy Management** section in the left part of the window.
3. Click the **Report** button in the right part of the window.
4. In the window that opens, a detailed report will be displayed on all categories of the selected user account.

DATA ENCRYPTION

Data Encryption is designed for protecting confidential information against unauthorized access. At that, encrypted information is stored in a special container.

Container is an encrypted object created by the user with the Data Encryption function. Files and folders are moved into the container. To access the data stored in the container, you should enter a password. Additionally, Kaspersky Small Office Security must be installed on the computer.

To work with the data in the container, you must decrypt them. In this case, Kaspersky Small Office Security requests a password for access. After you have entered the password, the container is displayed in the system as a virtual removable drive onto which you can copy or move files and folders with data.

IN THIS SECTION:

Creating and connecting an existing container 161

Locking and unlocking access to the data in the container 162

Adding files into container 163

Configuring container 164

Creating shortcut for quick access to the container 165

CREATING AND CONNECTING AN EXISTING CONTAINER

To store encrypted data, you need to create a container. You can create a container on a local or removable drive.

A container can be created using the wizard. When creating a container, you need to specify its name, size, access password, and container file location.

This wizard consists of a series of screens (or steps) navigated using the **Back** and the **Next** buttons. To close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing buttons in the top part of the window.

You can also connect an existing container if it is unavailable on the computer you are currently using (for example, after the operating system is reinstalled, or if the container is copied from another computer). In this case, the container appears in the list but data access is locked. To work with the data stored in the container, you must decrypt them (see section "Locking and unlocking access to the data in the container" on page 162).

To create a container, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Data Encryption** button.

   This opens the **Data Encryption** window.
4. Click the **Create container** button.
5. The Encrypted Container Creation Wizard will be started. Let us take a closer look at the wizard's steps:

   a. Enter the name of the container, as well as its size and access password in the **Main settings** window.

   b. Specify the location of the container file in the **Location** window.

   c. Select a letter of virtual drive to connect this container, specify the advanced settings, if necessary, and confirm creation of the container with the specified settings in the **Summary** window.

To connect an existing container, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Data Encryption** button.

   This opens the **Data Encryption** window.
4. Click the **Connect container** button.
5. In the window that opens, specify the location of the container file.

LOCKING AND UNLOCKING ACCESS TO THE DATA IN THE CONTAINER

After you have created the container, data access is unlocked. If an existing container is connected, access to it is locked by default. To work with the data in the container, you must decrypt them. You can do that via Kaspersky Small Office Security interface or the Microsoft Windows context menu.

If the container is stored on a removable medium, you can configure automatic unlocking of access to the data in the container on drive connection.

After you have unlocked access to the container, the container is available for all computer accounts as a removable drive in the list of devices, so we recommend that you block access to the data (encrypt the data in the container), if you are not working with them. You can encrypt data in a container using the Kaspersky Small Office Security interface or via Microsoft Windows context menu.

To decrypt the data in the container using the application interface:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Data Encryption** button.

This opens the **Data Encryption** window.

4. Click the **Decrypt data** button.

5. In the window that opens, enter the settings for data decryption and confirm unlocking of access.

To decrypt the data via context menu:

1. Right-click to open the context menu of a file or shortcut to access the container (see section "Creating shortcut for quick access to the container" on page 165) on the desktop.

2. In the menu that opens, select **Decrypt data**.

To automatically unblock access to the data in the container at the connection of a medium:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Data Encryption** button.

   This opens the **Data Encryption** window.

4. Select the container, access to which was unlocked, and click the **Configure** button.

5. In the window that will open, enter the password to obtain access to the container.

6. In the **Container settings** window that opens, check the **Unlock container automatically** box.

To decrypt data via application interface:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Data Encryption** button.

   This opens the **Data Encryption** window.

4. Select the container, access to which was unlocked, and click the **Encrypt data** button.

To encrypt the data via context menu:

1. Right-click to open the context menu of the container file, or that of a desktop shortcut to access the container (see section "Creating shortcut for quick access to the container" on page 165) or that of a removable drive.

2. In the menu that opens, select **Encrypt data**.

ADDING FILES INTO CONTAINER

After data decryption (see section "Locking and unlocking access to the data in the container" on page 162) the container is displayed as a virtual removable drive within the system, being available to all the users of the operating system. You can open the container and place files and folders in it if you need to store them in encrypted form. To ensure data security, we recommend that you encrypt the data after finishing the operations. After that, you need to enter a password to obtain access to the encrypted data.

To open a container via the application interface:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Data Encryption** button.

   This opens the **Data Encryption** window.

4. Select the container, access to which is unblocked, and open it with a double-click.

5. Place in it the data you want to encrypt.

To open a container via the context menu, please do the following:

1. Right-click to open the context menu of the container file or the shortcut to access the container (see section "Creating shortcut for quick access to the container" on page 165) on the desktop.

2. Select the **Open container** item from the menu that opens.

CONFIGURING CONTAINER

You can change the container's name and the access password.

You can only change the settings for the container, access to which is unblocked.

To rename a container, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Data Encryption** button.

   This opens the **Data Encryption** window.

4. Select a container and click the **Configure** button.

5. In the window that will open, enter the password to obtain access to the container.

6. In the **Container settings** window that opens, specify the new name of the container.

To change the password for the container, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Data Encryption** button.

   This opens the **Data Encryption** window.
4. Select a container and click the **Configure** button.
5. In the window that will open, enter the password to obtain access to the container.
6. In the **Container settings** window that opens, click the **Change password** link.
7. In the **Change password** window that opens, fill in all fields.

CREATING SHORTCUT FOR QUICK ACCESS TO THE CONTAINER

To ease the management of data, you can create a desktop shortcut for quick access to the container. You can use the shortcut to quickly open the container, and encrypt and decrypt data irrespective of the actual location of the container file (if you have access to the container file from your computer). You can create a shortcut for quick access to the container during container creation or at any time after the creation of the container.

You can only create a shortcut for the container, access to which is unblocked.

To create a shortcut to access the container, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Data Encryption** button.

   This opens the **Data Encryption** window.
4. Select a container and click the **Configure** button.
5. In the window that will open, enter the password to obtain access to the container.
6. In the **Container settings** window that will open, click the **Create desktop shortcut** link.

MANAGEMENT CONSOLE

The Management Console functions are designed to control Kaspersky Small Office Security remotely from the administrator's workplace when installed on office network computers.

The network administrator can take the following actions via Management Console:

- analysis of protection level of networked computers;
- scan of the whole network or individual computers for threats;
- centralized update of anti-virus databases;
- modification of the protection settings for networked computers;

- control over the use of computers and the internet by employees (only in Kaspersky Small Office Security 2 for Personal Computer);
- data backup on networked computers;
- viewing of reports on security subsystems' operation.

For the correct operation of Management Console, the following conditions should be met:

- Management Console should be protected with the same administrator password on all computers.
- There should be no computers with identical names in the local network.
- If the Firewall has been installed and enabled on your computer (in addition to the Kaspersky Small Office Security Firewall), an incoming and outgoing allowing rules for Kaspersky Small Office Security should be added to it.
- Microsoft Windows settings "Network Discovery" and "File and printer sharing" should be enabled.

To launch Management Console, please do the following:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console Configuration Wizard** button to start the Management Console Configuration Wizard (see section "Configuring remote management" on page 166). At further startups, the Management Console Configuration Wizard will no longer be required to run the Management Console; instead you will need to enter the administrator's password.

IN THIS SECTION:

Configuring remote management 166

Scanning the office network for viruses and vulnerabilities 167

Updating databases on networked computers remotely 167

Enabling / disabling protection components on networked computers 168

Remote Web Policy Management 169

Running backup tasks on networked computers 169

Managing licenses on networked computers remotely 170

CONFIGURING REMOTE MANAGEMENT

Remote control is configured using the wizard.

This wizard consists of a series of screens (or steps) navigated using the **Back** and the **Next** buttons. To close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing buttons in the top part of the window.

To configure Management Console, please do the following:

1. Open the main application window.

2. Select the **Management Center** section in the left part of the window.

3. In the right part of the window, click the **Management Console Configuration Wizard** button to start the Management Console Configuration Wizard. We shall examine in more detail the steps in the Management Console Configuration Wizard:

   a. Enter or set the administrator password in the **Password protection** window.

   b. Select computers subject to remote control in the **Search for computers** window.

   c. Select the update mode for anti-virus databases in the **Update method** window.

   d. Confirm the settings you have selected in the **Summary** window.

SCANNING THE OFFICE NETWORK FOR VIRUSES AND VULNERABILITIES

Using Management Console, you can run a virus scan task remotely either for the whole network, or for an individual computer.

To scan the whole network for viruses, please do the following:

1. Open the main application window.

2. Select the **Management Center** section in the left part of the window.

3. In the right part of the window in the **Group tasks** section, click the **Scan network computers** button.

4. In the **Group start of scanning** window that opens, select the scan type and the computers you need to scan.

To scan an individual computer for viruses or vulnerabilities, please do the following:

1. Open the main application window.

2. Select the **Management Center** section in the left part of the window.

3. In the right part of the window, click the **Management Console** button.

4. In the window that opens, select a computer in the top part of the window and go to the **Scan** section.

5. In the right part of the window, select the required scan task.

UPDATING DATABASES ON NETWORKED COMPUTERS REMOTELY

Using Management Console, you can remotely manage the updating of Kaspersky Small Office Security on the networked computers.

You can select one of the following update modes:

- Independent update of the databases on the computers.

- Downloading updates from the chosen computer on the network. In this case, one of the networked computers should be selected as the update server. Other computers download updates from this server.

To change the update mode for the networked computers, please do the following:

1. Open the main application window.

2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console** button.
4. In the window that opens, click the **Settings** link in the top part of the window.
5. In the Management Console Configuration Wizard that opens, proceed to the **Update method** step and select the required update mode.

To select a computer as an update server, please do the following:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console** button.
4. In the top part of the window that opens, select a computer and go to the **Update** section.
5. Click the **Make an update server** button.

You can run an update task remotely either for the whole network, or for an individual computer.

To run update on all the networked computers, please do the following:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window in the **Group tasks** section, click the **Database updates** button.
4. In the **Group start of update** window that opens, select the computers on which you need to download the updates.

To run the update on an individual computer, please do the following:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console** button.
4. In the top part of the window that opens, select a computer and go to the **Update** section.
5. In the right part of the window, click the **Perform update** button.

ENABLING / DISABLING PROTECTION COMPONENTS ON NETWORKED COMPUTERS

Using Management Console, you can remotely turn on / off different protection components on the networked computers.

To turn on / off a protection component remotely, please do the following:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console** button.

4. In the window that opens, select the computer for which protection management is required, and go to the **Information** section.

5. In the right part of the window, select the **Protection components** item.

6. In the **Protection components** window that opens, enable / disable the required protection component by clicking the status icon to the right from the component name.

REMOTE WEB POLICY MANAGEMENT

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Using Management Console, you can remotely set restrictions and view the statistics of events related to the users' activities on the networked computers and on the Internet.

To configure Web Policy Management remotely, please do the following:

1. Open the main application window.

2. Select the **Management Center** section in the left part of the window.

3. In the right part of the window, click the **Management Console** button.

4. In the window that opens, select a computer in the top part of the window and go to the **Web Policy Management** section.

5. In the right part of the window, select an account and click the **Configure policies** button.

To view the statistics, please do the following:

1. Open the main application window.

2. Select the **Management Center** section in the left part of the window.

3. In the right part of the window, click the **Management Console** button.

4. In the window that opens, select a computer in the top part of the window and go to the **Web Policy Management** section.

5. In the right part of the window, select an account and click the **Report** button.

RUNNING BACKUP TASKS ON NETWORKED COMPUTERS

Using Management Console, you can remotely run backup tasks on the networked computers, as well as view the report on executed backup tasks and data restoration tasks.

To backup objects remotely, please do the following:

1. Open the main application window.

2. Select the **Management Center** section in the left part of the window.

3. In the right part of the window, click the **Management Console** button.

4. In the window that opens, select a computer in the top part of the window and go to the **Backup and Restore** section.

5. In the right part of the window, select a backup task and click the **Run** button.

   You can pause or stop the task execution, by using the corresponding buttons in the top part of the window.

To obtain a report on the execution of backup tasks and data restoration tasks, please do the following:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console** button.
4. In the window that opens, select a computer in the top part of the window and go to the **Backup and Restore** section.
5. Click the **View report** button.
6. In the **Report** window that opens, specify the event display settings.

MANAGING LICENSES ON NETWORKED COMPUTERS REMOTELY

Using Management Console, you can remotely check the license status on the networked computers, renew the license, or activate the application using a new license.

To manage the license on a networked computer, please do the following:

1. Open the main application window.
2. Select the **Management Center** section in the left part of the window.
3. In the right part of the window, click the **Management Console** button.
4. In the window that opens, select the computer for which you want to view the list of problems, and go to the **Information** section.
5. In the right part of the window that opens, select the **License management** item.
6. In the **License management** window that opens, take the required actions.

PASSWORD MANAGER

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

Password Manager stores and protects all your personal data (e.g. passwords, user names, Internet pager accounts, contacts, phone numbers, etc.). Password Manager sticks passwords and accounts to Microsoft Windows applications and web pages for which they are used. All information is stored in encrypted form in the Password Database, access to which is protected by a Master Password. This information is only available if the Password Database is unlocked. After launching a web page or application, Password Manager automatically enters the password, user name and other personal data. Thus, you need not remember all the passwords, you only need to remember one password.

Password Manager loads by default at system startup. This component is built in into the application which allows personal data to be managed directly from the application window.

Password Manager monitors the actions of applications with passwords and prevents the interception and theft of personal data. This component checks applications that use passwords or request them from other applications, before asking you to allow or forbid a suspicious action.

Additionally, Password Manager can:

- save and use your passwords (see page 184);
- find accounts, passwords, user names and other personal information in the Password Database (see page 185);
- generate strong passwords (see page 203) when registering new accounts;
- save all passwords on removable device (see page 204);
- restore Password Database from backup copy (see page 188);
- protect passwords from unauthorized access (see page 176).

To open Password Manager from the Kaspersky Small Office Security main window,

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.

To open the Password Manager from the context menu of the application icon,

select the **Password Manager** item from the context menu of the Password Manager icon.

You can also launch the Password Manager by double-clicking (see page 203) the Password Manager icon in the taskbar notification area.

IN THIS SECTION:

Password Manager interface 171

Password Database management 176

Application settings configuration 189

Creating strong passwords 203

Using the portable version of Password Manager 204

PASSWORD MANAGER INTERFACE

The **Password Manager** main window consists of three parts:

- a button for locking and unlocking the Password Database (see page 176);
- caption buttons for access to the main Password Manager functions: password creation, identity creation, Password Database management, application settings configuration, creation and synchronization of a portable version of the Password Manager (unavailable if the Password Database is locked);
- the Password Generator button (see page 203).

You can also use the following buttons and links:

- **Information** – switch to the page with information about the application at the Technical Support website.
- **Help** - view Password Manager help system;
- **Close** – close Password Manager.

IN THIS SECTION:

Notification area icon 172

Context menu of Password Manager 173

Password Database window 173

Application settings window 174

Caption Button 174

Plug-ins 175

Pointer 175

NOTIFICATION AREA ICON

Immediately after installing Password Manager, the application icon will appear in the Microsoft Windows taskbar notification area.

Depending on the situation, the Password Manager icon will take the following form:

- active (green) – Password Manager unlocked, access to personal data granted;
- inactive (red) – Password Manager locked, personal data inaccessible.

The following interface items are accessible by clicking the icon:

- context menu;
- Password Manager pointer.

CONTEXT MENU OF PASSWORD MANAGER

You can start general protection tasks from the context menu of the application icon located in the taskbar notification area of Microsoft Windows. The context menu of the application icon contains the following options:

- **Lock / Unlock** – allow or forbid access to your personal data.
- **Accounts** – quick access to the most frequently used accounts. The number of accounts in the Password Database is specified in brackets. The list of frequently used accounts is created automatically. The list is available if it is configured to be displayed in the context menu (see page 192). When the application is first launched, the list will not be available since no record will have been used.
- **Secure Memos** – quick access to private notes. The number of secure memos in the Password Database is specified in brackets.
- **Add** – add a new task to Password Manager:
  - **Account** – start the Add Account Wizard (see page 177);
  - **Secure memo** – switch to the Add Secure Memo window (see page 184);
  - **Identity** – switch to the Add Identity window (see page 183).
- **Password Manager** – switching to the main application window (see page 171).
- **Settings** – configure application settings.
- **Portable version** - launching Portable Version Creation Wizard (see page 204).
- **Password Generator** – creating strong passwords (see page 203).
- **Help** – view Kaspersky Small Office Security help system.
- **Exit** – close the application. When this option is selected, the application will be unloaded from the computer's RAM.

If the application is not unlocked, access to your personal data will be blocked. In this case, the context menu will only contain the following items: **Unlock**, **Password Generator**, **Help**, and **Exit**.

To open the context menu of the application icon,

hover over the Password Manager icon in the taskbar notification area with the cursor and right-click it with the mouse.

PASSWORD DATABASE WINDOW

The Password Database window consists of three parts:

- in the upper part of the window, you can select Password Manager functions and perform the main tasks;
- the middle part of the window contains a list of all accounts and other personal data, and enables you to manage your personal information;
- the lower part of the window contains links for managing the Password Database as a whole.

You can also use the search field in the upper part of the window. The search field helps you find the necessary information in the Password Database using a keyword.

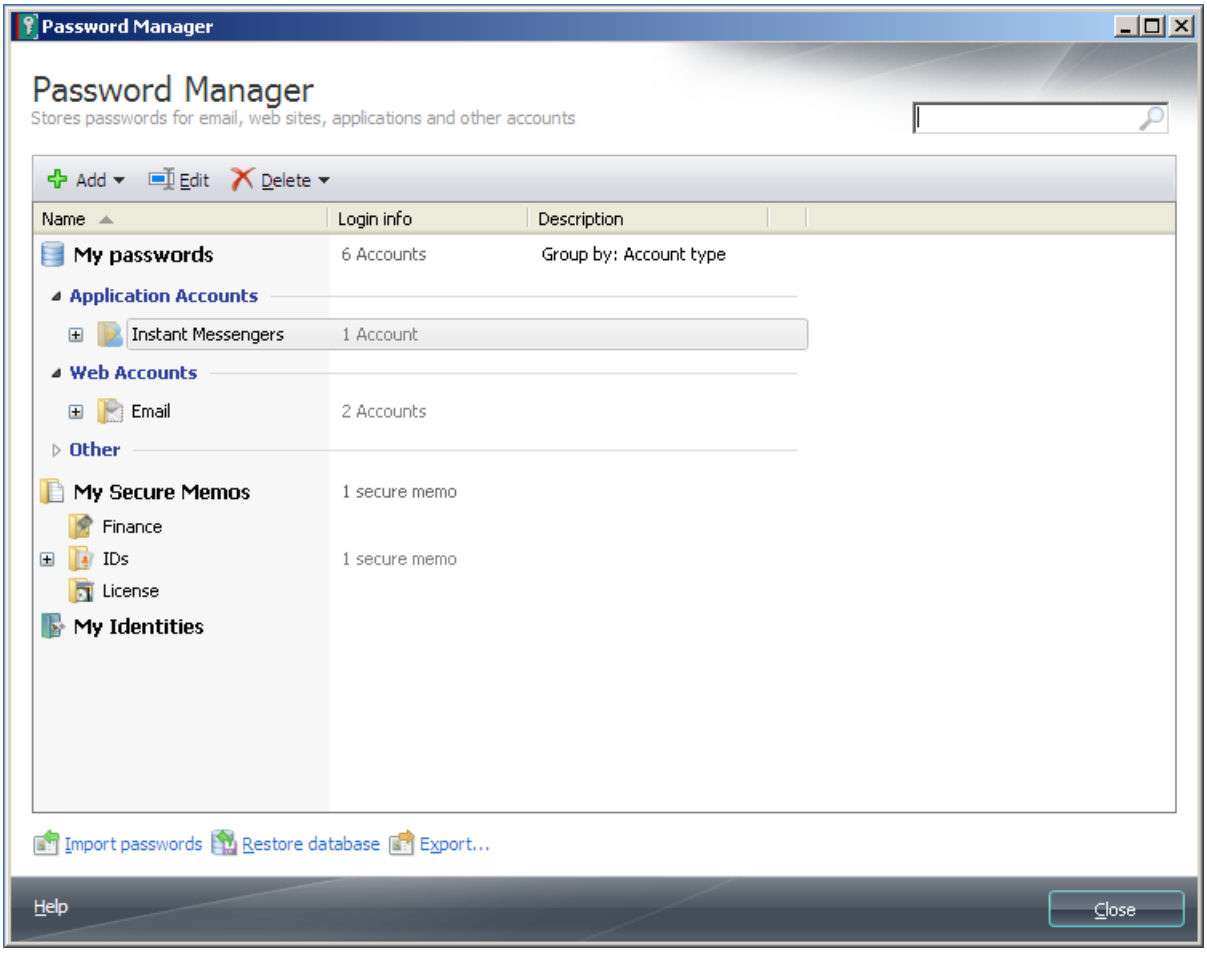

Figure 10. Password Database

APPLICATION SETTINGS WINDOW

The settings window in Password Manager can be opened in one of the following ways:

- from the context menu of Password Manager – to do so, select **Settings** in the context menu of Password Manager;
- from the Password Manager window – to do this, click the **Settings** button.

The application settings window consists of two parts:

- the left part of the window contains the list of application functions;
- the right part of the window contains the list of settings for the chosen function, task, etc.

CAPTION BUTTON

The Caption Button enables you to work with personal data from the application / browser window. This button is located in the upper-right corner of the application.

Clicking the Caption Button opens a menu with a list of user names that are related to the application / web page. When selecting a user name, Password Manager automatically fills in authorization fields using data from the Password Database.

The Caption Button is active if Password Manager is not locked (see page 176). Click it to do the following:

- **Add Account** – add a new account.
- **Edit Account** – add a user name / edit the activated account. The menu item is available if the account is activated.
- **Web Accounts** – view the list of all Web accounts and open one of them. The number of accounts in the Password Database is specified in brackets.
- List of frequently used accounts – launch an account from the list. The list is generated automatically based on how frequently the accounts are used. The list is available if it is configured to be displayed in the context menu (see page 192).
- **Identities** – view the list of created Identities and select an Identity for the registration form.
- **Password Manager Help** – switch to the application help system.

The Caption Button is not active if Password Manager is locked. In such case, clicking the button will not enable any actions. The inactive button is displayed in the application window if the settings of Caption Button are additionally configured (see page 201).

PLUG-INS

Password Manager has plug-ins embedded in applications that require authorization. You can install plug-ins independently for the browsers you need. Installed plug-ins provide access to Password Manager functions from the application / browser interface.

POINTER

Password Manager pointer lets you quickly choose the application / web page for automatic input of personal data.

To use the Password Manager pointer, please do the following:

1. Point the mouse cursor on the Password Manager icon the taskbar notification area and wait a few seconds.
2. When it appears, drag the Password Manager pointer to the required application / browser window. Password Manager automatically defines the action to be performed on the chosen application / web page.

PASSWORD DATABASE MANAGEMENT

The Password Database stores all accounts for applications and web pages with one or several user names, as well as Identities (cards containing, for example, contact details, phone numbers, Internet pager numbers, etc.).

You can use the Password Database if it is unlocked (see page 176). Before entering any changes in the Password Database, it is recommended that you configure the backup settings (see page 196). If this data is accidentally changed or deleted, use Restore Password Database (see page 188).

You can perform the following actions:

- add (see page 177), change, delete (see page 186) private data;
- import / export (see page 186), restore (see page 188) Password Database.

IN THIS SECTION:

Accessing Password Database 176

Adding personal data 177

Using personal data 184

Finding passwords 185

Deleting personal data 186

Importing / exporting data 186

Backup / restoring Password Database 188

ACCESSING PASSWORD DATABASE

To access the Password Database, select one of the following authorization methods:

- **Master Password protection**. Master Password is used to access the Password Database.
- **USB device**. To access the Password Database, connect any USB device to your computer. When the USB device is disabled, the Password Database is automatically locked.
- **Bluetooth device**. To access the Password Database, connect a Bluetooth device to your computer. When the Bluetooth device is disabled, the Password Database is automatically locked.
- **No authorization**. Access to the Password Database is unprotected.

By default, protection is set by the Master Password, which means that you only need to remember one password.

Master Password is the basic tool that protects your personal data. If you have selected the method of authorization with a device, and the latter has turned out to be unavailable (or lost), you can use the Master Password for accessing your personal data.

By default, Password Manager locks the Password Database when the application is launched and after a specified time during which the computer is not used (see page 198). The application can only be used if the Password Database is unlocked.

You can also unlock / lock the Password Database using one of the following methods:

- in the Password Manager window (see page 171);
- using a USB or Bluetooth device - only for authorization with a USB or Bluetooth device;
- by double-clicking the application icon (see page 203) - the double-click action in this case must be configured additionally;
- from the context menu of Password Manager;
- by pressing the **CTRL+ALT+L** shortcut (see page 194).

To enter the Master Password, use a virtual keyboard that allows passwords to be entered without pressing keys on the keyboard.

To lock an application from the context menu of the application, please do the following:

1. Right-click the Password Manager icon in the taskbar notification area.
2. In the menu that opens, select the **Lock** item.

To unlock the Password Database from the context menu, please do the following:

1. Right-click the Password Manager icon in the taskbar notification area.
2. In the displayed menu, select **Unlock**.
3. Enter the Master Password in the displayed window.

ADDING PERSONAL DATA

Personal data can be added if Password Database is not locked (see page 176). When launching an application / web page, a new account is recognized automatically if it was not found in the Password Database. Following authorization in the application / on the web page, Password Manager can then add personal data to the Password Database.

The following types of personal data are available in the Password Database:

- **Account**. Combination of a user name and password for authorization on the web page or in the program.
- **Group of accounts**. Used to organize accounts in the Password Database.
- **User name**. By default, Password Manager provides the option to create an account with one user name. An additional user name is used when applications or web pages allow multiple user names to be created for accessing their resources.
- **Identity**. Used to store data such as sex, date of birth, contact information, phone number, place of work, Internet pager number, homepage address, etc. To separate personal and business information, you can create several Identities.
- **Secure Memo**. Used to store any information.

ACCOUNT

Password Manager automatically recognizes a new account if it is not found in the Password Database. After authorization in the application / on the web page, Password Manager offers to save data in the Password Database. You can also add a new account to the Password Database manually.

Account contains the following data:

- type of account (application account or Internet account);
- user name / several user names;
- password;
- path to the application / Internet address of the web page (depending on the account type);
- settings which define relations between the account and the object;
- account activation settings;
- comments;
- settings for completing additional fields on the web page.

Password Manager lets you use one or several accounts for authorization in the program or on the web site.

Based on the path to the application or Internet address of the web page, Password Manager allows specifying a scope for each account.

You can add an account in several ways:

- by clicking the Caption Button – to do this, you need to select **Add Account** in the Caption Button menu;
- from the context menu of Password Manager – to do this, you need to select **Add** → **Account** in the context menu of the Password Manager icon;
- from the main Password Manager window.

To add a new account from the main window:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. In the top part of the window that opens, click the **Add** button and select the **Add Account** item.
6. In the Account Creation Wizard that opens, select the type of account (Web Account, Application Account or expert mode):
   - If you have selected an Internet account or an application account, click the **Next** button.

     At the next step in the Account Creation Wizard, specify the website or application that the account is to be used for, and click the **Next** button.
   - If you have selected the advanced mode, click the **Next** button.
7. At the next step in the Account Creation Wizard, specify the account settings:
   - In the top part of the **Account Name** field, enter or edit the name of the new account.
   - Under the tab **Login information**, enter the user name (login) and password.

     The user name can consist of one or several words. To specify key words (see page 179) for the user name, click .

To copy a user name / password to the clipboard, click the button.

To copy a user name from another account, follow the **Use shared Login from another Account** link.

To create a password automatically, open the Password Generator window by clicking the **Generate password** link (see page 203).

- Under the **Links** tab, specify the path to the program / web page, and specify the account's settings.
- On the **Manual form edit** tab, modify the settings for populating other fields of the web page, if necessary.
- If necessary, under the **Comments** tab, enter some explanatory text for the account. To display comments in a notification after activating the account, check the **Show comments in the notification** box.

8. Click the **Add Account** button.

KEYWORD SEARCH

To quickly search for personal data in the Password Database, you can use keywords. They are generated for each user name. It is recommended to assign keywords when adding an account (see page 177) / user name (see page 183).

To specify keywords for the user name, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Select a user name in the **My passwords** list, and in the top part of the window, click the **Edit** button.
6. On the **Login information** tab in the open window, click the button next to the **User name** field and type in the key words in the **Description** field.

ADDING PATH TO PROGRAM / WEB PAGE

To connect an account to an application or a web page, you should create a link. For a web page, a link is a web address. For an application, a link is a path to the executable application file on the computer. Without this data the account will not be sticked to any application / web page.

It is possible to stick the account to a program / web page in the following ways:

- by following the link in the list of your browser's chosen websites or the list of applications on your computer;
- by manually specifying the path to the application / web page;
- by using the Password Manager pointer.

To check the entered path, launch the application / web page by clicking .

To select a link from the list, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.

5. Select an account from the **My passwords** list and click the **Edit** button.

6. In the displayed window, under the **Links** tab, in the field **Link**, click .

7. In the displayed window, in the field **Link,** enter the path for the application / web page.

   To specify a web page from the list of saved web pages (Favorites), in the **Bookmarks** list, and click the **Copy link from Favorites** link. To copy the path to the web page from the browser window, click the **Use path to the linked application** link.

   To create a link to the application, in the **Link** field click the button and specify the path to the executable application file.

To specify the path to the program / web page manually, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Password Manager** button.

4. In the **Password Manager** window that opens, click the **Password Database** button.

5. Select an account from the **My passwords** list and click the **Edit** button.

6. In the displayed window, under the **Links** tab in the field **Link,** enter the path to the program / address of the web page. The address of the web page must begin with http://www.

To enter the path to the program / web page using the Password Manager pointer, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Password Manager** button.

4. In the **Password Manager** window that opens, click the **Password Database** button.

5. Select an account from the **My passwords** list and click the **Edit** button.

6. In the displayed window, under the **Links** tab, in the field **Link**, enter the path to the program / web page by moving the Password Manager pointer to the program / browser window.

SELECTING A METHOD TO STICK THE ACCOUNT

To determine which account data should be entered automatically at each startup of the application / web page, Password Manager uses the path to the application / Internet address of web page.

Because Password Manager allows using several accounts for a single application / website, you should specify a scope for each account.

Based on the path to the application / Internet address of web page, Password Manager allows creating a scope for any account. Scope may be configured at the account creation (see page 177). You can alter the settings in the future.

Depending on the object (application or website), the way accounts are used varies.

The following options are available for the application:

- Use the account for the application. The account will be used for all application's dialogs which have fields for entering personal data.

- Recognize by window heading. The account will only be used for the given application window.

For example, one application can use multiple accounts. For different accounts, only the window headings will differ within one application. Password Manager will automatically enter data for the account based on the application window's heading.

The following options for using an account are available for web pages:

- Only for the given web page. Password Manager automatically adds the user name and password to the identification fields on the given web page only.

  For example, if the account is related to a web page with the address http://www.web-site.com/login.html, it will not be valid for other websites, e.g. http://www.web-site.com/pointer.php.

- For websites from a directory. Password Manager automatically adds the user name and password to identification fields for all web pages in the most recent folder.

  For example, if the website address http://www.web-site.com/cgi-bin/login.html was entered, the account will be used for web pages in the *cgi-bin* folder.

- For the website: <third-level domain name and lower>. This account is used for any web page in the domain (third-level domain and lower).

  For example, Password Manager automatically adds identity data for websites: http://www.domain1.domain2.web-site.com/login.html or http://www.domain1.domain2.web-site.com/pointer.php. However, the account will not be used for web pages with addresses that have different fourth-level domains: http://www.domain3.domain2.web-site.com/pointer.php or http://www.domain4.domain2.web-site.com/pointer.php.

- For the website: <name of website>. The account will be used for all web pages with fields for entering user names and passwords.

  For example, Password Manager automatically adds identity cards for web pages: http://www.domain1.domain2.web-site.com/login.html, http://www.domain2.domain2.web-site.com/pointer.php, http://www.domain3.domain2.web-site.com/pointer.php or http://www.domain4.domain2.web-site.com/pointer.php.

To set parameters for using an account, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Select an account from the **My passwords** list and click the **Edit** button.
6. In the window that opens, under the **Links** tab, select one of the options for using the account.

AUTOMATIC ACTIVATION OF THE ACCOUNT

By default, automatic activation of the account is enabled. Password Manager only enters the user name and password in the identity fields. You can set additional activation parameters of the account (see page 177).

A range of web addresses, for which automatic activation is used, is additionally specified for the web page.

The following options are available for activating the account:

- For the chosen web page. The account is activated only for the given web page.
- For the website. The account is activated on all web pages on the website.

To set automatic activation of the account, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Select an account from the **My passwords** list and click the **Edit** button.
6. In the window that opens, on the **Links** tab, check the **Automatically activate Account after loading** box.

   Additionally, specify one of the methods to activate the account for the web page.

FILLING IN ADDITIONAL FIELDS

During authorization on a website, other data is often requested in addition to password and user name. Password Manager can automatically fill in additional fields. You can set options for automatic fill-in of additional fields for the account.

It is possible to set options for additional fields if the application path / website address is specified.

To set options for fields, Password Manager temporarily loads the website, and analyzes all the fields and buttons. Fields and buttons are merged into groups for each web page.

Password Manager temporarily saves files and pictures on your computer from the loaded web page.

To set options for additional fields, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Select a user name from the **My passwords** list and follow the **Edit** button.
6. In the window that opens, on the **Manual form edit** tab, follow the **Edit form fields** link.
7. In the top part of the **Manual form edit** window, check the box next to the required field or button.
8. Activate the field in the **Value** column for the chosen field or button with a double-click, and set the field values.

CREATING A GROUP OF ACCOUNTS

Using groups of accounts can help organize information in the Password Database. A group consists of a folder with accounts added to it.

Newly created groups are displayed in the Password Manager context menu: the **Accounts** → **<Group name>** item.

To create a group of accounts, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.

4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Select the line **My passwords** in the list of accounts.
6. In the top part of the window, click the **Add** button and select the **Add Group** item.
7. Enter the name of the new group.
8. Add accounts from the **My passwords** list by dragging them into the created group folder.

USER NAME

Multiple user names are often used for certain applications / websites. Password Manager allows multiple user names to be saved for one account. Password Manager automatically recognizes a user name when it is first used and provides the option to add it to an account for an application / website. You can add a new user name manually for an account and then change it. You can also use the same user name for different accounts.

You can add a new user name for an account in the following ways:

- By clicking the Caption Button. To do so, in the Caption Button menu, select the **Edit Account** → **Add Account** item.
- From the main application window.

To add a user name for an account, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Select an account from the **My passwords** list, click the **Add** button and select the **Add Account** item.
6. In the window that opens, enter the user name and the password. The user name can consist of one or several words. To specify keys words for a user name, click and then fill in the **Description** field.

   To copy a user name / password to clipboard, click . To create a password automatically, follow the **Generate password** (see page 203).

   To copy a user name from another account, follow the **Use shared Login from another Account** link.

IDENTITY

In addition to user name and password, other personal data is often used for registration on the website, e.g. full name, year of birth, sex, email address, phone number, country of residence, etc. Password Manager can store all this data in an encrypted Password Database in the form of Identities. During registration on a new website, Password Manager automatically fills in the registration form using data from a chosen Identity. To save private and business information separately, you can use several identities. You can change the Identity parameters later.

To create an Identity, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.

5. Click the **Add Identity** button in the top part of the window.
6. In the window that opens, in the **Name** field, enter the name of the identity.
7. Enter values for the required fields and activate them by double-clicking the mouse in the **Value** column.

SECURE MEMO

Secure memos are designed for storing text information in encrypted from (for example, passport data, bank account data, etc.), and for quick access to the saved data. Password Manager includes a set of standard text editor tools to help you edit the text of Secure memo. When creating a Secure memo, you can use templates with a set of standard types of data (see page 200).

You can change the settings of Secure memo in the future.

- *To create a Secure memo from scratch, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Click the **Create Secure Memo** button in the top part of the window.
6. In the window that opens, in the **Name** field, enter the name of Secure memo.
7. Enter the necessary information in the text editor.

- *To create a Secure memo based on a template, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Click the **Create Secure Memo** button in the top part of the window.
6. In the window that opens, in the **Name** field, enter the name of Secure memo.
7. In the bottom part of the window, click the **Select template** button and select the required template.
8. Fill in the required data and format the text, if necessary.

- *To view the Secure memo,*

  open the context menu of Password Manager and select **Secure Memos** → **<Name of group>** →**<Name of Secure memo>**.

USING PERSONAL DATA

Password Manager sticks accounts to applications / web pages for which they are used. Password Database automatically searches for sticky accounts when applications / web pages are launched. If an account is found, personal data is entered automatically. If there is no sticky account in the Password Database, Password Manager automatically suggests adding an account to the Password Database (see page 177).

Some applications / websites can use multiple user names. Password Manager allows several user names to be saved for one account. If a new user name was used during authorization, Password Manager suggests adding it to the account (see page 183) for the application or web page that was launched. When the application / web page is next launched, a window with a list of user's names for this account will appear next to the personal data input fields.

In addition to the user name and password, other personal data is often used on the website for registration (e.g. full name, sex, country, town/city, phone number, email address, etc.). Password Manager can store this data in an encrypted Password Database in the form of Identities. To separate private and business information, you can create several Identities (see page 183). When you register in the program / on the web site, Password Manager will automatically use the chosen card to fill in the registration form. Using Identities saves time completing identical registration forms.

During authorization in the application / on the web page, Password Manager automatically enters personal data only if the Password Database is unlocked.

An account can be used in the following ways:

- Launch application / web page. The authorization form will be filled automatically using data from the account.
- Use Password Manager pointer. To do this, move the mouse cursor over the application icon in the taskbar notification area, then activate the account by dragging the Password Manager pointer to the required application / browser window.
- Select the account from the list of frequently used accounts. To do this, open the context menu of Password Manager and under frequently used accounts, select the required record.
- Use context menu of Password Manager. To do so, open the Password Manager context menu and select the **Accounts** → **<Account name>** item.

To use an Identity, please do the following:

1. Click the Caption Button in the upper-right corner of the application / browser window.
2. In the menu that opens, select the **Identities** → **<Identity name>** item. Password Manager automatically fills in the registration fields on the web page using data from the Identity.

FINDING PASSWORDS

A search for personal data could be hindered in the following cases:

- Some passwords are not associated with applications / websites.
- Password Database contains a large number of accounts.

Password Manager quickly finds passwords by the following parameters:

- account name;
- user name;
- key words (see page 179) (key word search parameters are set additionally for each user name);
- address (for web pages).

The search is performed both by full name, and by initial letters and any characters included in the account name or link.

To find an account / password, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. In the top part of the window, enter the text in the search field.

DELETING PERSONAL DATA

Before making any changes to personal data, Password Manager automatically creates a backup copy of the Password Database. If this data is accidentally changed or deleted, use Restore Password Database (see page 188). From the Password Database it is possible to delete one or all elements.

- *To delete an element from the Password Database, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Select an item from the **My passwords** list, click the **Delete** button and choose **Delete**.

- *To delete all elements from the Password Database, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Select an item from the **My passwords** list, click the **Delete** button and choose **Delete all**.

IMPORTING / EXPORTING DATA

Password Manager can import and export your Password Database, and individual objects within Password Database (Identities, user accounts, and Secure memos).

You can import both passwords from other password management applications (e.g. Internet Explorer, Mozilla Firefox, KeePass), and passwords that you have exported using Password Manager earlier. Passwords are imported from *.xml and *.ini files.

Password Manager can export the Password Database to *.xml, *.html or *.txt files. Exporting passwords to a file is convenient for opening general access passwords, printing the Password Database, or saving a backup copy of the Password Database to a file in a different format to Password Manager.

Exported passwords are stored in unencrypted files and are not protected from unauthorized access. Therefore, it is recommended to consider ways of protecting exported files in advance.

When imported, the Password Database is modified. You can choose one of the following actions to be performed on the Password Database:

- **Overwrite**. The current Password Database will be replaced with the imported one (all passwords stored in Password Manager's Password Database before import will be deleted).
- **Merge**. The imported passwords will be added to the Password Database. When merging, you are given the option of importing accounts into Password Manager.
- **Cancel**. The import of passwords will be cancelled.

To import passwords from a file, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Click the **Import** link in the lower part of the window o open the **Import passwords** window.
6. In the **Import passwords** window that opens, select the application, from which passwords will be imported, and click the **Import passwords** button.
7. In the window that opens, specify the file with passwords that you wish to import, and click **Open**.
8. In the window that opens, select the required action to be performed on the Password Database.

To save the Password Database to a file, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. Run the Data Export Wizard by clicking the **Export** link in the lower part of the window.
6. In the Data Export Wizard window that opens, select export mode (exporting the entire Password Database or selected objects) and click **Next**.
7. At the next step in the Data Export Wizard, select the export settings:
   - If you want to protect the data you are exporting, select **Secure export** and specify the password for data protection.
   - If you want to export your data to an unprotected file, select **Export without encryption** and specify the file format for exporting.
   - To schedule a change of password for exported data, select the **Use a reminder date if you want to be notified about expiration of exported items** checkbox and choose the date when the password expires. Password Manager will inform you of the need to change the password.
8. Click the **Next** button.
9. At the next step in the Data Export Wizard, specify the path to export the file and click the **Next** button.
10. At the next step in the Data Export Wizard, verify the export settings for your data and click the **Export** button.

BACKUP / RESTORING PASSWORD DATABASE

Before any changes are made to Password Database, a backup copy is automatically created. The path of the reserve copy is set by default, but you can change it (see page 196). It is useful to restore passwords in the following cases:

- if the most recent changes need to be cancelled;
- if the Password Database was overwritten or deleted;
- if the current Password Database is inaccessible / damaged after a hardware or system failure.

All data in the backup copy is stored in encrypted form. Password Manager registers all changes to the Password Database. In the application, backup copies are displayed in a list and sorted according to date, beginning with the most recent. For each backup copy, the following data is provided:

- location;
- date and time of creation;
- changes made relative to the previous version.

You can use backup copies to solve the following tasks:

- restore a Password Database from a backup copy;
- delete copies of a backup storage;
- change the location of backup copies (see page 196).

To restore the Password Database, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. In the bottom part of the window, click the **Restore database** link.
6. In the **Restore** window that opens, select the date of a backup copy from the list, and in the top part of the window click **Restore**.
7. In the window, confirm the restoration by clicking **OK**.

To remove unnecessary backup copies, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. In the bottom part of the window, click the **Restore database** link.
6. In the **Restore** window that opens, in the list of backup copies, select the versions of backup copies to delete. To select several versions, hold the **CTRL** key.

7. Click **Delete**.

8. In the window that opens, confirm data deletion by clicking **OK**.

APPLICATION SETTINGS CONFIGURATION

Configuration of application settings is possible if Password Database is unlocked (see page 176). When editing the settings, you can do the following:

- set the time when the application is launched;
- enable notifications (see page 202);
- specify the user name (see page 191) that will be used by default when creating a new account;
- set the time when the password was stored in clipboard (see page 202);
- create a list of frequently used accounts (see page 192);
- create a list of ignored websites (see page 193), for which Password Manager functions are not used;
- create a list of trusted websites (see page 193) for which Password Manager will allow readdressing;
- specify a key combination to quickly launch Password Manager functions (see page 194);
- change the path for storing Password Database (see page 194), backup copies (see page 196);
- change data encryption method (see page 196);
- set automatic locking of Password Database (see page 198);
- change Master Password (see page 199);
- configure access to the Password Database (see page 198);
- change the location of Caption Button, create a list of applications supporting Caption Button (see page 201);
- create a list of supported applications (see page 200).

To edit Password Manager settings, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the **Password Manager Configuration** window, select the section to be edited.
6. In the right part of the window, enter the changes to the settings for the chosen section.

IN THIS SECTION:

Configuration Wizard 190
Default user name 191
Frequently used accounts 192
Ignored web addresses 193
Trusted web addresses 193
Hot keys 194
Location of the Password Database file 194
Creating new Password Database 195
Location of the backup copy 196
Selecting encryption method 196
Automatic locking of Password Database 198
Changing Password Manager authorization method 198
Using USB-, Bluetooth-devices for authorization 198
Changing Master Password 199
Supported web browsers 200
Managing Secure memos templates 200
Displaying Caption Button 201
Time when the password was stored in the clipboard 202
Notifications 202
Double-click action 203

CONFIGURATION WIZARD

The configuration wizard for the application is launched when Password Manager is started for the first time. Its purpose is to help you perform the initial configuration of Password Manager in accordance with your personal preferences and tasks.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Close** button.

STEP 1. CREATING MASTER PASSWORD

Password manager uses a Master Password to protect all your personal data. A Master Password is configured at the first startup of the application. Do not use as a password the data that are easy to guess (for instance, surnames, names, dates of birth). To ensure a strong password, use upper and lower case characters, figures and symbols.

The Master Password grants you the access to all personal data. Remember that losing one of your passwords can result in losing all your passwords.

Enter the Master Password in the **Master Password** field, and then in the **Confirm Master Password** field. To protect the password against interception, you can enter the password using the Virtual Keyboard; open it by clicking the **Virtual Keyboard** option.

Check the **I have read the information below about the importance of my Master Password** box.

You can change Master Password later (see page 199).

STEP 2. CHOOSING AUTHORIZATION METHOD

Authorization enables to control access to your personal data. You can use one of the following authorization methods:

- **Password protection**. To unlock the Password Database, you must enter the Master Password. This is the default authorization method.
- **USB device**. To access the Password Database, connect any USB device to your computer. For example, flash cards, cameras, MP3 players, and external hard drives can be used as a USB device. When the USB device is disabled, the Password Database is automatically locked.
- **Bluetooth device**. To access the Password Database, use a Bluetooth device. Bluetooth must be enabled on both the mobile phone and the computer which uses Password Manager. When connecting a mobile phone and computer via Bluetooth, the Password Database will be unlocked. If the link drops (e.g. you disable Bluetooth on the mobile phone), the Password Database will be locked.
- **Without authorization (not recommended)**. Access to the database will be unprotected. Your personal data will be available for all users who work on your computer.

If you select authorization using a USB or Bluetooth device, you are recommended to remember your Master Password. If there is no authorization device available, Password Manager enables the use of Master Password for access to your personal data.

You can change the authorization method198 later (see page).

STEP 3. LOCKING PASSWORD MANAGER

Password Manager automatically locks the password database after launching an application and when the computer has not been used for some time. You can specify the time interval after which the password database will be blocked.

By default, after application startup the password database is always blocked. If the computer is used by several users, it is recommended to switch on the automatic block. Check the **Ask Master Password at Password Manager startup** box for the Password Manager to automatically offer you to enter the Master Password to unlock the database.

You can change the condition for locking Password Database later (see page 198).

STEP 4. CLOSING THE WIZARD

At the final step, the Installation Wizard notifies you that Password Manager has been successfully installed. To complete the Wizard, click the **Finish** button.

DEFAULT USER NAME

Password Manager allows a user name to be set that will be automatically displayed in the **User name** field when creating a new account (see page 177).

To set the default user name, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window that opens, select the **General** section.
6. In the right part of the window, fill in the **Default Login** field.

FREQUENTLY USED ACCOUNTS

Password Manager provides quick access to accounts. The list of frequently used accounts is displayed in the main application window. It can also be displayed in the context menu and in the Caption Button menu. This list contains the names of applications / web pages that you run most frequently. Items in the list are arranged in alphabetical order or by frequency of use.

The list of frequently used accounts is available in the menu if Password Database is not locked (see page 176).

You can set the following list options:

- **Number of items in the list** – maximum number of frequently used accounts that are displayed in the context menu of the application;
- **Display list in application menu** – the list of frequently used accounts will be accessible in the context menu of Password Manager;
- **Display in the Caption Button menu** – the list of frequently used accounts will be accessible in the Caption Button menu (from the application / browser window).

To display frequently used accounts in the context menu, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **Frequently used Accounts** section.
6. In the right part of the window, check the **Show the list in the system tray menu** box.

   To display the list of frequently used accounts in the Caption Button menu, additionally check the **Display in the Caption Button menu** box.

   If the **Show the list in the system tray menu** box is not checked, the remaining options in the list cannot be modified.

7. Specify the number of accounts in the **List size** field.
8. If necessary, modify the items in the list manually. To remove an item from the list, select the required account in it, and click **Delete**. To delete all items from the list, click **Clear**.

IGNORED WEB ADDRESSES

You can specify a list of web addresses for which Password Manager will not be used. Automatic input of user name and password is disabled for websites on this list. Besides, Password Manager will automatically abstain from offering you to create a new account (see page 177) / user name (see page 183) for those websites.

To create a list of ignored web addresses, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **Ignored web addresses** section.
6. In the right part of the window, click **Add**, enter the web address and press **ENTER**.

   To change a web address, select it from the list and click **Edit**. To delete a web address from the list, select it and click **Delete**.

TRUSTED WEB ADDRESSES

Password Manager protects your personal data from phishing attacks. If during authorization you were redirected to another website, the application will notify you about it.

Phishers often use redirecting to websites that give access to bank accounts (e.g. Internet banking sites, payment systems, etc.). On the company's official authorization page, users are redirected to a counterfeit website visually similar to the official page. All data entered on the counterfeit page falls into the hands of attackers.

Redirecting is often officially installed on websites. If you don't want Password Manager to consider readdressing to be a phishing attack, you can create a list of trusted web addresses. The list of trusted web addresses includes websites to which the entered personal data are transferred. During authorization, Password Manager will not notify you of the personal data being transferred to a trusted website.

Password Manager allows transferring personal data to trusted websites from other websites. Before adding a website to the list of trusted web addresses, make sure it is completely reliable.

You can add a website to the list of trusted web addresses in the following ways:

- directly during authorization on the website;
- manually, from the **Password Manager Configuration** window.

To add a website to the list of trusted web addresses during authorization on the website, wait to be redirected from one website to the other, and then, in the Password Manager window, select the check box **Always trust <name of website>**.

To create a list of trusted web addresses manually, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.

5. In the left part of the window, select the **Trusted web addresses** section.

6. In the right part of the window, click **Add**. The field in the **Trusted web addresses** list will become active. Then, enter the web address and press **ENTER**.

   To change the web address, select it in the list and click **Edit**. To delete the web address from the list, select it in the list and click **Delete**.

HOT KEYS

To quickly access certain application functions, it is convenient to use hotkeys.

You can specify hotkeys for the following actions:

- Lock / Unlock Password Manager (see page 176).
- Enter the password.

To access functions quickly, you can specify one key or a combination of two or three keys.

Avoid key combinations used by Microsoft Windows to access functions.

To specify a shortcut, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **Hot keys** section.
6. In the right part of the window, set the required key combination for each action.

LOCATION OF THE PASSWORD DATABASE FILE

Password Manager's Password Database is an encrypted file (see page 196) that stores all your personal data (accounts, user names, passwords, and Identities).

The default paths for different versions of Microsoft Windows are as follows:

- Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\;
- Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\;
- Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\.

You can use different media to store your Password Database: removable disk, local disk, or network drive.

The following actions are possible when changing the path or names of the Password Database:

- **Copy** – creates a copy of the Password Database with the specified path. This copy will become an active Password Database.

- **Move** – the active Password Database will be saved in the specified location.
- **Create new Password Database** – creates an empty copy of the Password Database that will become active.

To move or rename the Password Database, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **My passwords** section.
6. In the right part of the window under **Location**, click located in the right part of the **Path** field.
7. In the **Select Password Database** window, specify the name and path of the file and click the **Open** button.
8. In the **Password Database location** window that opens, select the necessary action to be performed on the Password Database.
9. In the **Password Manager** window, enter the Master Password to confirm the changes.

To change the current Password Database, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **My passwords** section.
6. In the right part of the window under **Location**, click located in the right part of the **Path** field.
7. In the **Select Password Database** window, select the Password Database file and click the **Open** button.
8. In the **Password Manager** window that opens, enter the Master Password to access the chosen Password Database.

CREATING NEW PASSWORD DATABASE

Password Manager allows the use of several Password Databases. Creating a new Password Database allows your personal data to be separated and saved in two or more Password Databases. If necessary, an old Password Database can be restored. Password Manager can create a new Password Database if the current Password Database is damaged or cannot be restored from a backup copy.

To create a new Password Database, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.

5. In the left part of the window, select the **My passwords** section.
6. In the right part of the window under **Location**, click located in the right part of the **Path** field.
7. In the **Select Password Database** window, specify the location and filename of the Password Database and click **Open**.
8. In the **Password Database location** window that opens, select the **New Password Database** action.
9. In the **New Password Database** window, under **Password**, set the password for access to the new database and re-enter it in the field **Confirm password**.

   If the password is re-entered incorrectly, it will be highlighted red.

   Under **Encryption algorithm** select the encryption provider and required encryption method (see page 196).
10. In the displayed window, enter the new Master Password to confirm creation of a new Password Database.

LOCATION OF THE BACKUP COPY

Before saving any changes to your personal data, Password Manager automatically makes backup copies of the Password Database. This avoids any losses of data in the event of system or technical failure. Password Manager creates a complete copy of the Password Database before implementing the changes. If the Password Database is damaged, you can restore data from the most recent backup copy of the Password Database (see page 188).

You can use different media to store the backup copy of your Password Database: local disk, removable disk, or network drive.

By default, depending on the operating system, the backup copy is saved with the following path:

- Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\;
- Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\;
- Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\.

To change the path of the backup file, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **My passwords** section.
6. In the right part of the window, under **Backup**, click the button located in the right part of the field **Path**.
7. In the **Browse For Folder** window, select the folder for the backup copy of the Password Database.

SELECTING ENCRYPTION METHOD

The task of cryptography is to protect information from unauthorized access and distribution. The main purpose of the cipher is to transfer encrypted messages via unprotected channels.

Keys are required for encryption and decryption. A key is a vital component of a cipher. If one and the same key is used for encryption and decryption, it is called a symmetric key. If two keys are used , it is asymmetric. Symmetric ciphers can be either block or stream. Any information (regardless of the format of the source data) is interpreted in binary code. A block cipher assumes all data will be broken into blocks, each of which will then undergo an independent transformation. In a stream cipher, the algorithm is applied to each bit of information.

Password Manager offers the following symmetric algorithms:

- **DES**. Block cipher with the standard-sized key of 56 bit. By today's standards, DES does not offer a high level of protection. This algorithm is used when reliability is not the main requirement.
- **3DES**. A block algorithm created based on DES. It solves the main weakness of its predecessor – the small key size. 3DES keys are three times the size of those used by DES (56*3=168 bits). The speed of operation is three times slower than for DES, but the level of security is much higher. 3DES is used more often, since DES is not resilient enough against modern cracking techniques.
- **3DES TWO KEY**. A block algorithm created based on DES. This is a 3DES algorithm which uses a key size of 112 bits (56*2).
- **RC2**. A block-cipher algorithm with variable-length key quickly processes a large amount of information. It is a faster algorithm than DES. In terms of security and resilience, it is comparable to 3DES.
- **RC4**. A stream cipher with variable-length key. The key size can range from 40 to 256 bits. The advantages of the algorithm are its high speed and variable key size. By default, Password Manager uses RC4 to encrypt data.
- **AES**. A block-cipher symmetric algorithm with a key length of 128, 192, 256 bits. This algorithm guarantees a high level of security and is one of the most commonly used.

Microsoft Windows uses an encryption provider to perform cryptographic operations. Each encryption provider supports several encryption algorithms with a specified key length. Password Manager uses the following built-in Microsoft Windows encryption providers:

- Microsoft Base Cryptographic Provider;
- Microsoft Enhanced Cryptographic Provider;
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype);
- Microsoft RSA/Schannel Cryptographic Provider;
- Microsoft Strong Cryptographic Provider.

To change the encryption algorithm, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **My passwords** section.
6. In the right part of the window, under **Encryption**, click **Change**.
7. In the **Encryption algorithm** window that opens, specify the encryption settings.

AUTOMATIC LOCKING OF PASSWORD DATABASE

Password Manager automatically locks the Password Database after launching an application and after a specified time during which the computer was not used. You can specify the time interval after which the Password Database will be locked. The value of the interval varies from 1 to 60 minutes. It is recommended that the Password Database be locked after 5-20 minutes of computer inactivity. You can also disable the automatic blocking of Password Database.

Password Manager automatically locks the Password Database after a set period of computer inactivity. If automatic locking of the computer is disabled, your personal data will not be protected if you leave your computer without locking it manually.

To modify the interval after which the Password Database becomes locked, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **My passwords** section.
6. In the right part of the window, under **Automatic locking**, use the drop-down list to select the time after which Password Database will be locked.

   To disable the locking of Password Database, select **Never**.

CHANGING PASSWORD MANAGER AUTHORIZATION METHOD

Authorization enables to control access to your personal data. You choose the authorization method at the first startup of the Password Manager (see page 191), but if necessary, the authorization method can be changed.

To change the authorization method, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **Authorization method** section.
6. In the right part of the window, under **Authorization method**, select an authorization option from the drop-down list.

USING USB-, BLUETOOTH-DEVICES FOR AUTHORIZATION

To access the Password Database (see page 198), Password Manager allows the use of various USB and Bluetooth devices.

To use a USB device to access the Password Database, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **Authorization method** section.
6. In the right part of the window, under **Authorization method**, select the **USB device** value from the drop-down list.
7. Connect the removable device to the computer.
8. Select a device from the **Disk drives** list and click **Set**. The icon appears next to the chosen device. If the connected device does not appear in the list, check the **Show additional devices** box. If necessary, you can change the authorization device by clicking **Reset**.

To use a Bluetooth device to access the Password Database, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **Authorization method** section.
6. In the right part of the window under **Authorization method**, select the value **Bluetooth device** from the drop-down list.
7. Enable Bluetooth on your computer, and then on the device.
8. Select a device from the **Phones and modems** list, and then click **Set**. The icon appears next to the chosen device. If necessary, you can change the authorization device by clicking **Reset**.

CHANGING MASTER PASSWORD

Master Password is created when Password Manager is launched for the first time (see page 190). You can change it later.

When changing the Master Password, Password Manager requests confirmation of the input password (the new password should be entered again). The new password cannot be saved without confirmation. If the confirmation password does not match the entered password, the confirmed password will be highlighted red. In this case, a warning message will appear when you try to save the new password.

To change the Master Password, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **Authorization method** section.

6. In the right part of the window, under **Password protection**, click **Change**.

7. In the **Password protection** window that opens, enter the new password in the **Password** and **Confirm password** fields.

SUPPORTED WEB BROWSERS

To ensure that automatic activation of the account and the Caption Button (see page 201) are working correctly, for several browsers and mail clients Password Manager requests the installation of additional extensions (plug-ins). By default, plug-ins are installed when Password Manager is first launched. You can install additional plug-ins.

The Password Manager contains a list of web browsers and mail clients, where each program is assigned the status, **Installed** or **Not installed** depending on whether or not the required plug-in is installed.

It is recommended to close all programs for which the plug-in will be installed.

To install a plug-in for a browser or mail client, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Password Manager** button.

4. In the **Password Manager** window that opens, click the **Settings** button.

5. In the left part of the window, select the **Supported browsers** section.

6. In the right part of the window, select a program from the list of **Supported browsers and available extensions**, then click **Install**.

7. Follow the instructions of the **Setup Wizard**. Once the plug-in is installed, the program will automatically move to the **Installed** group. It will be assigned the **Installed** status. You can delete an installed plug-in by clicking **Uninstall**.

MANAGING SECURE MEMOS TEMPLATES

You can edit preset templates of Secure memos (see page 184), create new templates, use as a template an existing Secure memo.

To change a preset Secure memo template, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Password Manager** button.

4. In the **Password Manager** window that opens, click the **Settings** button.

5. Select the **Manage templates** section in the left part of the window.

6. In the right part of the window, select a template from the list and click the **Edit** button.

7. Make the necessary changes in the text editor.

To create a Secure memo template, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. Select the **Manage templates** section in the left part of the window.
6. In the right part of the window, click **Add**.
7. In the window that opens, in the **Name** field, enter the name of a new Secure memo template.
8. Enter the necessary information in the text editor.

To use an existing Secure memo as a template, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Password Database** button.
5. In the window that opens, select the required Secure memo from the list, and in the top part of the window, click the **Edit** button.
6. In the bottom part of the window that opens, click the **Save as template** button.
7. In the window that opens, in the **Name** field, enter the name of a new Secure memo template.

DISPLAYING CAPTION BUTTON

If, in addition to the Program Manager menu, the application you are working with has other embedded application menus, you can set the position of the Caption Button in relation to the other buttons. Besides, it is possible to generate a list of browsers for which the Caption Button is used.

To change the Caption Button display settings, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **Caption Button** section.
6. In the right part of the window, under **Caption Button display**, set the required parameters in accordance with the task:
   - to change the location of the Caption Button, in the **Move button to the left** field, enter the position number of the button (how many buttons will be located to the right of the Caption Button);

- to prevent the Caption Button from being displayed when locking the Password Database, check the **Do not display if Password Manager is locked** box;

- to create a list of browsers in which the Caption Button is available, in the **Caption Button in web browsers** section, check the box next to the required browser from the list.

TIME WHEN THE PASSWORD WAS STORED IN THE CLIPBOARD

Password Manager can copy the password to the clipboard for a specified period of time. This is convenient for quick actions with passwords (e.g. when you need to use a created password to register on a website / in an application). You can set the amount of time the password will be saved in the clipboard. When this time expires, the password is automatically deleted from the clipboard. This will prevent the interception and theft of passwords because they will not be able to be copied from the clipboard when the specified time expires.

To change the backup time of the password in the clipboard, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **General** section.
6. In the right part of the window, under **Clipboard**, set the time in seconds.

NOTIFICATIONS

When Password Manager is running, various events occur that are of an informational nature. To keep up to date, use the notifications service. Users are notified of events by prompts and pop-up messages.

The following types of notifications are implemented in the application:

- **Application start**. A message appears upon application restart, when the application has already been started and the Password Database is not locked.

- **Account activation**. A message appears when the account is activated.

- **Clear clipboard**. Password Manager can temporarily store the password in clipboard. This is convenient when data needs to be copied and then pasted in the selected field. When specified time expires (see page 202), the password will be deleted from clipboard.

- **Password Manager autolocking**. The message appears when Password Manager automatically blocks the password database. By default, Password Manager automatically locks the Password Database after the operating system starts up and after a specified time (see page 198), during which the computer is not used.

- **Exporting passwords to unencrypted file**. A warning message saying that after export, your passwords will be saved in a non-encrypted file, and will consequently be made accessible to any user working on your computer. We recommend that before exporting data you consider ways of protecting the file containing passwords.

- **Manual form edit**. To set parameters for additional fields, the application requests permission to use the default browser. The message warns that images and system files (cookies) will be saved on your computer.

- **Difficulties populating login information for the Account**. This message warns that personal data cannot be entered automatically during authorization.

To receive notifications, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **General** section.
6. In the right part of the window, click the **Notification settings** button in the **General** section.
7. In the displayed window, check or uncheck the box next to the required types of notifications.

DOUBLE-CLICK ACTION

The Password Manager allows you to select an action, which will be performed by double-clicking the application icon in the Microsoft Windows taskbar notification area (see page 172). You may select one of the following actions:

- open the main window of Password Manager (see page 171);
- lock / unlock Password Manager (default action).

To set the task to be launched by double-clicking the application icon in the taskbar notification area, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Password Manager** button.
4. In the **Password Manager** window that opens, click the **Settings** button.
5. In the left part of the window, select the **General** section.
6. In the right part of the window, select the action from the drop-down list **On double-click**.

CREATING STRONG PASSWORDS

Data security depends directly on the strength of the passwords. Data could be at risk in the following cases:

- one password is used for all accounts;
- the password is simple;
- the password uses information that is easy to guess (e.g. family members' names or dates of birth).

To ensure data security, Password Manager allows unique and reliable passwords to be created for accounts using Password Generator.

A password is considered strong if it consists of more than four characters and contains special symbols, numbers, and upper- and lower-case letters.

Password security is determined by the following parameters:

- **Length** – the number of symbols in the password. This value can range from 4 to 99 symbols. The longer the password, the stronger it is considered to be.
- **A-Z** – uppercase letters.
- **a-z** – lowercase letters.
- **0–9** – numbers.
- **Special symbols** – special symbols.
- **Exclude similar symbols** – the use of identical symbols in a password is not permitted.

To create a strong password using the Password Generator, please do the following:

1. Open the context menu of Password Manager and select **Password Generator**.
2. In the **Password Generator** window, specify the number of symbols in the password in the **Password length** field.
3. If necessary, you can specify additional settings for Password Generator under **Additional** by checking / unchecking the box next to the required settings.
4. Click **Generate**. The created password is displayed in the **Password** field. To view the created password, check the **Show password** box.
5. Paste the password to clipboard by using the button , then enter the password in the password input field in the application / on the web page by pressing **CTRL+V**. The created password is saved in the clipboard.
6. To save the specified settings for subsequent use, check the **By default** box.

USING THE PORTABLE VERSION OF PASSWORD MANAGER

Password Manager allows storing all your passwords on a removable medium (e.g., a flash card or a cell phone if it is used as flash card). To do so, you should create a portable version of the Password Manager on a removable device. The application's portable version is created on the computer where the full version of Kaspersky Password Manager has been installed. The portable version of the application features the full functionality of Password Manager.

The portable version allows using Password Manager on a public computer (for example, in a cybercafé or a library), where the Password Manager is not installed. As soon as a removable device is connected to the computer, Password Manager starts up automatically. As soon as a removable device is disabled, Password Manager automatically closes and removes all of your data from the public computer.

Besides, you can use the portable version to synchronize your Password Databases, if Password Manager is installed and is used simultaneously on several computers (for example, on your home computer and in your office).

IN THIS SECTION:

Creating and connecting the portable version 204

Password Database synchronization 205

CREATING AND CONNECTING THE PORTABLE VERSION

For the portable version of Password Manager to run correctly on a public computer, you are recommended to install additional plug-ins for your web browser.

A plug-in can be installed in one of the following ways:

- From the plug-in installation wizard's window. To do so, follow the steps of the plug-in installation wizard at the first launch of the portable version of Password Manager.

- From the Caption Button menu in the web browser window. To do so, in the Caption Button menu, select the **Kaspersky Password Manager autofill plug-in is not installed** item.

At the first launch of the application on the public computer, the installation wizard of the Password Manager's portable version starts automatically. You are offered to apply the following advanced settings to the usage of the application's portable version:

- create a shortcut of the portable version on the desktop, which allows launching the application later from the desktop of this computer;

- use Virtual Keyboard – opens the virtual keyboard to enter personal data.

To create a portable version of Password Manager, please do the following:

1. Open the main application window.

2. In the left part of the window, select the **Tools** section.

3. In the right part of the window, click the **Password Manager** button.

4. In the **Password Manager** window, click the **Portable version** button.

5. In the Portable Version Creation Wizard window that opens, select the device on which you wish to install the portable version of Password Manager, and click **Next**. If the connected device does not appear in the list, check the **Show additional devices** box.

6. At the step, configure the portable version:

   - To not enter the Master Password for access to the portable version of Password Manager, select the **Never request Master Password** box.

   - For the Portable Version to start automatically at the connection of a removable device to the computer, select the **Enable Autorun of Password Manager from removable device** checkbox.

7. Click the **Run** button. Click **Finish** when the installation is complete.

To use the application's portable version, please do the following:

1. Connect the removable device to the computer.

2. Run the portable version of the Password Manager from the selected removable drive, if it did not start automatically at the connection of a medium.

3. At the first launch of the portable version, you will be offered to install autofill plug-ins, and disable the integrated password managers for the web browsers installed on your computer.

4. Enter the Master Password in the displayed window.

   The portable version of Password Manager is ready for use.

PASSWORD DATABASE SYNCHRONIZATION

If you use Password Manager on different computers, you need to keep all Password Databases up to date. Using the portable version, you can synchronize the data and use the up-to-date Password Database on all computers where Password Manager is installed. To do that, synchronize the Password Database of the portable version with the Password Database on one computer, and then synchronize it again on another computer.

To synchronize the Password Database of the portable version with the Password Database on one of the computers, please do the following:

1. Connect the removable device to the computer.
2. Open the main application window.
3. In the left part of the window, select the **Tools** section.
4. In the right part of the window, click the **Password Manager** button.
5. In the **Password Manager** window, click the **Portable Version** button.
6. In the Portable Version Creation Wizard window that opens, select the device on which you wish to install the portable version of Password Manager, and click **Next**. If the connected device does not appear in the list, check the **Show additional devices** box.
7. At the next step in the Portable Version Creation Wizard, select the method to synchronize the Password Database:
   - To add the data from the Password Manager's database installed on the computer to the Password Database of the portable version, select the **Merge Password Databases** option.

     The database of the Password Manager installed on the computer will not be changed. To add the merged data, repeat synchronization, by selecting the **Use the Portable Version database** option.

     At the next step of the Portable Version Creation Wizard, clear the check boxes opposite the records that are not to be included in the merged password database, and click the Next button.
   - To replace the Password Database of the Portable Version by the Password Database of the Password Manager installed on your computer, select the **Use the database of Password Manager installed on this computer option**.
   - To replace the Password Database of the Password Manager installed on the computer with the Password Database of the portable version, select the **Use the Password Database of the Portable Version** option.
8. Click the **Next** button.
9. At the next step of the Portable Version Creation Wizard, configure the portable version:
   - To not enter the Master Password for access to the portable version of Password Manager, select the **Never request Master Password** box.
   - For the Portable Version to start automatically at the connection of a removable device to the computer, select the **Enable Autorun of Password Manager from removable device** checkbox.
10. Click the **Run** button. Click the **Finish** button when the synchronization is complete.

PERFORMANCE AND COMPATIBILITY WITH OTHER APPLICATIONS

Performance of Kaspersky Small Office Security is implied as the range of detectable threats as well as energy consumption and resource intensity.

Kaspersky Small Office Security allows you to flexibly configure the protection scope and select various types of threats (see section "Selecting detectable threat categories" on page 207), that the application should detect.

Energy consumption has a great importance for portable computers. Scanning computers for viruses and updating Kaspersky Small Office Security databases often require significant amounts of resources. Special laptop mode of

Kaspersky Small Office Security (see page 209) allows you to automatically postpone scheduled scan and update tasks when using batteries, thus saving battery charge.

Consumption of the computer's resources by Kaspersky Small Office Security may impact other applications' performance. To solve problems of joint operations with increased load of the CPU and disk subsystems, Kaspersky Small Office Security may pause scan tasks and concede resources to other applications (see page 208) running on your computer.

In Presentation Mode, the application automatically disables displaying notifications of Kaspersky Small Office Security's activity with other applications running in full-screen mode.

In case of an active infection in the system, the advanced disinfection procedure requires restarting your computer, which may also impact other applications' performance. If necessary, you can disable the advanced disinfection technology (see page 207) to avoid an unwanted restart of your computer.

IN THIS SECTION:

Selecting detectable threat categories 207

Advanced disinfection technology 207

Distributing computer resources when scanning for viruses 208

Application settings in full-screen mode. Presentation Mode 208

Battery saving 209

SELECTING DETECTABLE THREAT CATEGORIES

Threats detected by Kaspersky Small Office Security are divided into categories by various attributes. The application always detects viruses, Trojan programs, and malicious utility tools. These programs can do significant harm to your computer. To ensure more reliable computer protection, you can extend the list of detected threats by enabling control of actions performed by legal applications that may be used by an intruder to do harm to the user's computer and data.

To select the detectable threat categories:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Threats and Exclusions** subsection.
4. In the right part of the window, in the **Threats** section click the **Settings** button.
5. In the **Threats** window that opens, check the boxes for the categories of threats that should be detected.

ADVANCED DISINFECTION TECHNOLOGY

Today's malicious programs can invade the lowest levels of an operating system which makes them practically impossible to delete. If a malicious activity is detected within the system, Kaspersky Small Office Security offers you to carry out a special advanced disinfection procedure which allows elimination of the threat and deletes it from the computer.

After this procedure, you will need to restart your computer. After restarting your computer, you are advised to run full virus scan (see section "How to perform full scan of your computer for viruses" on page 46).

For Kaspersky Small Office Security to use the advanced disinfection procedure:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Compatibility** subsection.
4. In the right part of the window, check the **Enable Advanced Disinfection technology** box.

DISTRIBUTING COMPUTER RESOURCES WHEN SCANNING FOR VIRUSES

Virus scan tasks may be postponed to limit the load on the central processing unit (CPU) and disk storage subsystems.

Executing scan tasks increases the load on the CPU and disk subsystems, thus slowing down other applications. By default, if such a situation arises, Kaspersky Small Office Security pauses virus scan tasks and releases system resources for the user's applications.

However, there is a number of applications which start immediately when CPU resources become available, and run in the background. For the scan not to depend on the performance of those applications, system resources should not be conceded to them.

Note that this setting can be configured individually for every scan task. In this case, the configuration for a specific task has a higher priority.

For Kaspersky Small Office Security to postpone scan tasks when they slow down other applications:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Compatibility** subsection.
4. In the right part of the window, check the **Concede resources to other applications** box.

APPLICATION SETTINGS IN FULL-SCREEN MODE. PRESENTATION MODE

Certain programs running in full-screen mode are marginally compatible with some features of Kaspersky Small Office Security: for example, pop-up notifications are really undesirable in that mode. Quite often those applications require significant system resources, meaning that running certain Kaspersky Small Office Security tasks may slow down their performance.

To avoid manually disabling notifications and pausing tasks every time you launch full-screen applications, Kaspersky Small Office Security provides the option of temporarily changing the settings using the Presentation Mode. When the Presentation Mode is active, switching to full-screen mode automatically changes the settings of all product components to ensure optimal system functioning in that mode. Upon exit from the full-screen mode, product settings return to the initial values used before entering the full-screen mode.

To enable the Presentation Mode, please do the following:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **General Settings** section, select the **Presentation Mode** subsection.

4. In the right part of the window, select the **Use Presentation Mode** check box, and in the **Presentation Mode settings** section, specify the required settings for Presentation Mode.

BATTERY SAVING

To save power on a portable computer, virus scan and scheduled update tasks can be postponed. If necessary, you can update Kaspersky Small Office Security or start a virus scan manually.

To enable the power conservation mode and extend battery life:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **General Settings** section, select the **Power Saving** subsection.

4. In the right part of the window, check the box **Disable scheduled scans while running on battery power**.

KASPERSKY SMALL OFFICE SECURITY SELF-DEFENSE

Because Kaspersky Small Office Security ensures your computer protection against malware, malicious programs penetrating your computer, attempts to block Kaspersky Small Office Security or even delete the application from your computer.

Stable performance of your computer's security system is ensured by features of self-defense and protection against remote access implemented in Kaspersky Small Office Security.

Kaspersky Small Office Security self-defense prevents modification and deletion of own files on the hard disk, processes in the memory, and entries in the system registry. Protection against remote access allows you to block all attempts to remotely control application services.

On computers running under 64-bit operating systems and Microsoft Windows Vista, Kaspersky Small Office Security self-defense is only available for preventing the application's own files on local drives and system registry records from being modified or deleted.

IN THIS SECTION:

Enabling and disabling self-protection 209

Protection against external control 210

ENABLING AND DISABLING SELF-PROTECTION

By default, Kaspersky Small Office Security self-defense is enabled. You can disable self-defense, if necessary.

To enable or disable Kaspersky Small Office Security self-protection:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **General Settings** section, select the **Self-Defense** subsection.

4. In the right part of the window, uncheck the **Enable Self-Defense** box, if Kaspersky Small Office Security self-protection should be disabled. Check this box if you need to enable self-defense.

PROTECTION AGAINST EXTERNAL CONTROL

By default, protection against external control is enabled. You can disable protection, if necessary.

Frequent are situations when remote administration programs (such as RemoteAdmin) are needed while using the remote access protection. To ensure performance of these applications, you should add them to the list of trusted applications (see section "Creating a list of trusted applications" on page 137) and enable the **Do not monitor application activity** setting for them.

To disable protection against external control:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **General Settings** section, select the **Self-Defense** subsection.

4. In the right part of the window, in the **External control** section, uncheck the **Disable external service control** box.

APPLICATION APPEARANCE

You can change the appearance of Kaspersky Small Office Security, using alternate skins. Also, the use of various active interface elements can be configured (such as the application icon in the Microsoft Windows taskbar notification area, or pop-up messages).

IN THIS SECTION:

Active interface elements 210

Kaspersky Small Office Security skin 211

News Agent 211

ACTIVE INTERFACE ELEMENTS

You can configure the display of active interface elements, such as notification windows or the Kaspersky Small Office Security icon in the toolbar.

To configure active interface elements:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the left part of the window, in the **General Settings** section, select the **Appearance** subsection.

4. In the right part of the **Icon in the taskbar notification area** block, check or uncheck the required boxes.

KASPERSKY SMALL OFFICE SECURITY SKIN

All colors, fonts, icons and texts used in Kaspersky Small Office Security's interface can be modified. You can create your own skins for the application, or localize application interface in another language.

To use another application skin:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Appearance** subsection.
4. Check the **Use alternative skin** box in the right part of the window section to activate a skin. Specify the folder with the skin settings in the entry field or click the **Browse** button to find this directory.

NEWS AGENT

Using *News Agent*, Kaspersky Lab informs you of all important events related to Kaspersky Small Office Security and protection against computer threats.

The application notifies you of the latest news by displaying a pop-up message in the taskbar notification area. In this case, the application icon changes its shape (see below).

You can read the news in one of the following ways:

- click the icon in the taskbar notification area;
- click the **Read news** link in the pop-up news message.

To disable news delivery:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Appearance** subsection.
4. In the right part of the window, under **Icon in the taskbar notification area**, uncheck the **Enable news notifications** box.

ADDITIONAL TOOLS

The following wizards and tools included with Kaspersky Small Office Security are used to resolve specific issues concerning your computer's security:

- Rescue Disk Creation Wizard is designed to create the Rescue Disk that allows you to restore the system operability after a virus attack by booting the computer up from removable media. Rescue Disk should be used when the infection is at such a level that it is deemed impossible to disinfect the computer using anti-virus applications or malware removal utilities.
- Privacy Cleaner Wizard is designed for searching and eliminating traces of a user's activities in the system, and the operating system's settings which allow the gathering of information about user activities.
- Unused Data Clearing Wizard is designed for searching and eliminating temporary and unused files on your computer and optimization of the system's functioning.
- System Restore Wizard is designed to eliminate system damage and traces of malware objects in the system.
- Browser Configuration Wizard – designed to analyze and adjust the settings of Microsoft Internet Explorer in order to eliminate its potential vulnerabilities.
- Permanently Delete Data Wizard ensures annihilation of confidential data without any opportunity of restoring them in the future.

All the problems found by the Wizards (except the Rescue Disk Creation Wizard) are grouped based on the type of danger they pose to the operating system. Kaspersky Lab offers a set of actions for each group of problems which help eliminate vulnerabilities and weak points in the system's settings. Three groups of problems and, respectively, three groups of actions on them, when detected, are distinguished:

- *Strongly recommended actions* will help eliminate problems posing a serious security threat. You are advised to perform in time all the actions in this group to eliminate the threat.
- *Recommended actions* help eliminate problems posing a potential threat. You are advised to perform all actions in this group as well to provide the optimal level of protection.
- *Additional actions* help repair system damages which do not pose a current threat but may threaten your computer's security in the future. Performing these actions ensures comprehensive protection of your computer. However, in some cases, they may lead to deletion of user settings (such as cookies).

IN THIS SECTION:

Permanently Delete Data 212

Privacy Cleaner 213

Delete Unused Data 215

Browser Configuration 216

PERMANENTLY DELETE DATA

Data security is ensured not only by the protection against viruses, Trojans and other types of malware, but also by the protection against unauthorized restoration of deleted information.

Deleting data with the standard Microsoft Windows tools cannot ensure safety and prevent possible restoration. The data do not disappear from the hard drive when deleted. They are stored in the disk sectors and marked as free. The file record in the file table is the only thing which is deleted. Formatting data storage media (such as hard disk drives, flash

cards, or USB cards) cannot guarantee total data deletion either. It is considered that data can only be deleted after multiple re-recording. However, even in this case, information may be restored using high-performance software tools.

Kaspersky Small Office Security includes the Permanent Data Deletion Wizard. This wizard allows deleting confidential data without any opportunity of restoring and using them by hackers. Permanent data deletion precludes from restoring information using common software tools. The wizard is applicable both to small-sized objects and to large-sized ones (up to several gigabytes).

The wizard supports deletion of data from the following data storage media:

- Local drives. Deletion is possible if the user has the rights required for recording and deleting information.
- Removable drives or other devices that can be detected as removable drives (such as floppy disks, flash cards, USB cards, or cell phones). Data can be deleted from a flash card if the mechanic protection from rewriting (Lock mode) is disabled.

Before starting the permanent deletion, the application finds out if data can be deleted from the selected data storage medium. The deletion procedure can only be carried out if the selected data storage medium supports data deletion. Otherwise, the data cannot be deleted permanently.

You can only delete the data that you can access under your personal account. Before deleting the data, make sure that the file or the folder is not opened, or it is not in use by other applications.

Such objects as a file or a folder can be deleted. To avoid unintentional deletion of useful data, you can select only one object for deletion, although the folder you have selected for deletion may contain several files or nested folders.

The folder you have selected for deletion may contain system files that cannot be deleted on penalty of operating system failures. When system files and folders are found among the chosen data, the wizard requests additional confirmation for their deletion.

Methods for permanent deletion of personal data are standardized. They are based on multiple rewriting deleted information with ones, zeroes, or random symbols. Deletion speed and quality may vary depending on the number of cycles.

To delete data without any opportunity of restoring them:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Additional Tools** button.
4. In the window that opens, click the **Permanently Delete Data** button.
5. In the **Permanently Delete Data** window that opens, select an object using the **Browse** button, then select an object to delete in the **Select folder** window that opens.

   From the **Data deletion method** dropdown list, select the required data deletion algorithm.
6. In the window that opens, confirm the data restoration by clicking **OK**. If some files are not deleted, try to delete them again by clicking the **Retry** button in the window that opens. To select another object to delete, click the **Finish** button.

ELIMINATING ACTIVITY TRACES

When working with the computer, a user's actions are registered in the system. Saved data include the search queries entered by users and visited web sites, launched programs, opened and saved files, Microsoft Windows system event log, temporary files, etc.

All these sources of information about the user's activity may contain confidential data (including passwords) and may become available to intruders for analysis. Frequently, the user has insufficient knowledge to prevent information being stolen from these sources.

Kaspersky Small Office Security includes the Privacy Cleaner Wizard. This Wizard searches for traces of user activities in the system as well as for operation system settings, which contribute to the storing of information about user activity.

Please keep in mind that the data related to user activity in the system are accumulated all the time. The launch of any file, or the opening of any document is logged. The Microsoft Windows system log registers many events occurring in the system. For this reason, repeated running of the Privacy Cleaner Wizard may detect activity traces which were not cleaned up by the previous run of the Wizard. Some files, for example the Microsoft Windows log file, may be in use by the system while the Wizard is attempting to delete them. In order to delete these files, the Wizard will suggest that you restart the system. However, during the restart, these files may be re-created and detected again as activity traces.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the Privacy Cleaner Wizard:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Additional Tools** button.
4. In the window that opens, click the **Erase Your Activities History** button.

The Wizard steps in detail.

Step 1. Starting the Wizard

Make sure the **Diagnostics of user activity traces** option is selected and click the **Next** button to start the Wizard.

Step 2. Activity signs search

This Wizard searches for traces of malware activities in your computer. The scan may take some time. Once the search is complete, the Wizard will proceed automatically to the next step.

Step 3. Selecting the Privacy Cleaner actions

When the search is complete, the Wizard displays the detected activity traces and actions suggested to eliminate them. The Wizard activity report is displayed as a list (see section "Additional Tools" on page 212).

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

It is strongly recommended not to uncheck the boxes selected by default because doing so will leave your computer vulnerable to threats.

Having defined the set of actions, which the Wizard will perform, click the **Next** button.

Step 4. Privacy Cleaner

The Wizard will perform the actions selected during the previous step. The elimination of activity traces may take some time. To clean up certain activity traces, computer restart may be required; the Wizard will notify you about that.

Once the clean-up is complete, the Wizard will proceed automatically to the next step.

Step 5. Closing the Wizard

If you wish to clean up the traces of user activity automatically whenever Kaspersky Small Office Security completes work, use the last screen of the Wizard to check the box **Clean activity traces every time on Kaspersky Small Office Security exit**. If you plan to remove the activity traces manually using the Wizard, do not check this box.

Click the **Finish** button to close the Wizard.

DELETE UNUSED DATA

The system may often accumulate too many temporary or unused files which reduces its performance. Temporary and unused files often require too large amounts of memory. Additionally, they may be exploited by malicious programs.

The temporary files are created at the launch of any applications or operating systems. But some of them remain undeleted when closing the application or operating system.

Unused information includes the following files:

- system event logs, where the names of all active applications are recorded;
- event logs of various applications (such as Microsoft Office, Microsoft Visio, Macromedia Flash Player) or update utilities (such as Windows Updater, Adobe Updater);
- system connection logs;
- temporary files of Internet browsers (cookies);
- temporary files remaining after installation / removal of applications;
- Recycle Bin contents;
- files in the TEMP folder whose volume may grow up to several gigabytes.

Kaspersky Small Office Security includes the Unused Data Clearing Wizard. The wizard's purpose is helping you optimize the system's functioning. Besides the deletion of unused files from the system, the wizard deletes the files which may contain confidential data (passwords, usernames, data from registration forms). However, for complete deletion of such data, we recommend using the Privacy Cleaner Wizard (see page 213).

When cleaning the system, some files (such as Microsoft Windows log file, Microsoft Office event log) may be in use by the system. In order to delete these files, the Wizard will suggest that you restart the system.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the Unused Data Clearing Wizard, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Additional Tools** button.
4. In the window that opens, click the **Delete Unused Data** button.

The Wizard steps in detail.

Step 1. Starting the Wizard

Click the **Next** button to start the wizard.

Step 2. Searching for unused information

The wizard searches for temporary and unused files on your computer. The scan may take some time. Once the search is complete, the Wizard will proceed automatically to the next step.

Step 3. Selecting actions to delete unused files

When the search is complete, the Wizard displays the detected unused files and actions suggested to delete them. The Wizard activity report is displayed as a list (see section "Additional Tools" on page 212).

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

It is strongly recommended not to uncheck the boxes selected by default because doing so will leave your computer vulnerable to threats.

Having defined the set of actions, which the Wizard will perform, click the **Next** button.

Step 4. Delete Unused Data

The Wizard will perform the actions selected during the previous step. The deletion of unused information may take some time. To delete certain files, computer restart may be required; the Wizard will notify you about that.

Once the clearing of unused information is complete, the Wizard will automatically proceed to the next step.

Step 5. Closing the Wizard

Click the **Finish** button to close the Wizard.

BROWSER CONFIGURATION

Microsoft Internet Explorer browser requires in certain cases special analysis and configuring since some setting values selected by the user or set by default may cause security problems.

Here are some examples of the objects and parameters used in the browser and how they are associated with potential security threats:

- **Microsoft Internet Explorer cache**. The cache stores data downloaded from the Internet, which allows not to download them next time. This speeds up the download time of your web pages and reduces Internet traffic. In addition to that, the cache contains confidential data, from which a history of websites visited by the user can also be obtained. Some malware objects also scan the cache while scanning the disk, and intruders can obtain, for example, the user's email addresses. You are advised to clear the cache every time you close your browser to improve the protection.

- **Display of known file types extensions**. To edit file names conveniently you can disable showing their extensions. Nevertheless, it is sometimes useful to see the file extension. File names of many malicious objects contain combinations of symbols imitating an additional file extension before the real one (e.g., example.txt.com). If the real file extension is not displayed, users can see just the file name part with the

imitated extension and so they can identify a malicious object as a harmless file. To improve protection, you are advised to enable the display of files of known formats.

- **List of trusted web sites**. For some websites to run correctly, you should add them to the list of trusted sites. At the same time, malicious objects can add to this list links to websites created by intruders.

Note that some settings may lead to problems with displaying certain websites (for example if they use ActiveX controls). This problem can be solved by adding these websites to the trusted zone.

Browser analysis and configuration are performed in the Browser Configuration Wizard. The Wizard checks if the latest browser updates are installed and makes sure that the current browser settings do not make the system vulnerable to malicious exploits. Once the Wizard is complete, a report is generated which can be sent to Kaspersky Lab for analysis.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

Close all Microsoft Internet Explorer windows before starting the diagnostics.

To start the Browser Configuration Wizard:

1. Open the main application window.
2. In the left part of the window, select the **Tools** section.
3. In the right part of the window, click the **Additional Tools** button.
4. In the window that opens, click the **Tune Up your Browser Settings** button.

The Wizard steps in detail.

Step 1. Starting the Wizard

Make sure the **Microsoft Internet Explorer diagnostics** option is selected and click **Next** to start the Wizard.

Step 2. Microsoft Internet Explorer settings analysis

The Wizard analyzes Microsoft Internet Explorer browser settings. Searching the browser settings for problems may take some time. Once the search is complete, the Wizard will proceed automatically to the next step.

Step 3. Selecting actions to configure the browser

The problems found during the previous step are presented in groups, based on the type of danger that they pose (see section "Additional Tools" on page 212).

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

It is strongly recommended not to uncheck the boxes selected by default because doing so will leave your computer vulnerable to threats.

Having defined the set of actions, which the Wizard will perform, click the **Next** button.

Step 4. Browser Configuration

The Wizard will perform the actions selected during the previous step. Browser configuration may take some time. Once configuring is complete, the Wizard proceeds automatically to the next step.

Step 5. Closing the Wizard

Click the **Finish** button to close the Wizard.

REPORTS

Events that occur during the operation of the protection components or when the Kaspersky Small Office Security tasks are run, are logged in reports. You can create a detailed report for each protection component or task and configure display of data in the most convenient form. Additionally, you can filter data (see section "Data filtering" on page 219) as well as use search (see section "Events search" on page 219) through all events included in the report.

You can save report data (see section "Saving a report into a file" on page 220) to a text file, if necessary. You can also clear the reports (see section "Clearing application reports" on page 221) containing the data which are no longer useful, and adjust the settings for creating (see section "Logging non-critical events" on page 221) and storing (see section "Storing reports" on page 220) reports.

IN THIS SECTION:

Creating a report for the selected component 218

Data filtering 219

Events search 219

Saving a report to file 220

Storing reports 220

Clearing application reports 221

Logging non-critical events 221

Configuring the reminder of report availability 221

CREATING A REPORT FOR THE SELECTED COMPONENT

You can obtain a detailed report about events which occurred during the operation of each of the Kaspersky Small Office Security components or during execution of its tasks.

To work with the reports conveniently, you can change the data display on the screen: group events by various parameters, select the report period, sort events by column or by importance and also hide columns.

In order to create a report on a certain component or a task, perform the following steps:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Small Office Security.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.

   The **Detailed report** window opens.
4. In the top left part of the window, select in the dropdown list a component or task, for which a report should be created. When selecting the **Protection Center** item, a report is created for all protection components.

DATA FILTERING

You can filter events in the reports of Kaspersky Small Office Security by one or several values in the report columns and also define complex data filtering conditions.

To filter events by the values, perform the following steps:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Small Office Security.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.

   The **Detailed report** window opens.
4. In the right part of the window, move the mouse pointer to the upper left corner of the column header and click it to open the filter menu.
5. Select in the filter menu the value, which should be used to filter data.
6. Repeat the procedure for another column, if necessary.

To specify a complex filtering condition, perform the following steps:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Small Office Security.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.

   The **Detailed report** window opens.
4. In the right part of the window, right-click the appropriate report column to display the context menu for it and select **Filter by this field**.
5. In the **Custom filter** window that opens, specify the filtration conditions:

   a. Define the query limits in the right part of the window.

   b. In the left part of the window select from the **Condition** dropdown list the necessary query condition (e.g., is greater or less, equals or does not equal the value specified as the query limit).

   c. If necessary, add the second condition using logical conjunction (logical AND) or disjunction (logical OR) operations. If you wish your data query to satisfy both specified conditions, select **AND**. If only one of the two conditions is required, select **OR**.

EVENTS SEARCH

You can search a report for the necessary event using a keyword in the search line or special search window.

To find an event, please do the following:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Small Office Security.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.

   The **Detailed report** window opens.

4. Right-click to open the context menu of the appropriate column header and choose **Search**.
5. Specify the search criteria in the **Search** window that opens:
   a. In the **String** field, enter a key word to be searched for.
   b. In the **Column** dropdown list, select the name of the column that should be searched for the specified key word.
   c. If necessary, check the boxes for additional search settings.
6. Click the **Find next** button.

SAVING A REPORT TO FILE

The report obtained can be saved to a text file.

In order to save the report to file, perform the following actions:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Small Office Security.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.

   The **Detailed report** window opens.
4. Create the required report and click **Save**.
5. In the window that opens, select a folder into which you wish to save the report file, and enter the file name.

STORING REPORTS

The default maximum report storage duration is 30 days. Then the reports will be deleted. You can cancel the time-based restriction or change the maximum report storage duration.

Besides, you can also define the maximum report file size. By default, the maximum size is 1024 MB. Once the maximum size has been reached, the content of the file is replaced with new records. You can cancel any limits imposed on the report's size, or enter another value.

- *To modify the report maximum storage time:*

  1. Open the main application window.
  2. In the top part of the window, click the **Settings** link.
  3. In the left part of the window, in the **General Settings** section, select the **Reports and Storages** subsection.
  4. In the right part of the window, under **Storage**, check the **Store reports no longer than** box and specify maximum report storage duration.

- *To configure the maximum report file size, perform the following steps:*

  1. Open the main application window.
  2. In the top part of the window, click the **Settings** link.
  3. In the left part of the window, in the **General Settings** section, select the **Reports and Storages** subsection.
  4. In the **Storage** section in the right part of the window, check the **Maximum file size** box and specify maximum size for a report file.

CLEARING APPLICATION REPORTS

You can clear the reports containing data that you need no longer.

- *To clear* reports:

  1. Open the main application window.
  2. In the top part of the window, click the **Settings** link.
  3. In the left part of the window, in the **General Settings** section, select the **Reports and Storages** subsection.
  4. In the right part of the window, in the **Clear reports** section, click the **Clear** button.
  5. In the **Clearing reports** window that opens, check the boxes for the reports you wish to clear.

LOGGING NON-CRITICAL EVENTS

By default, the product does not add to its reports non-critical events, registry and file system events. You can add such records to the protection reports.

- *To include an entry into a log of non-critical events:*

  1. Open the main application window.
  2. In the top part of the window, click the **Settings** link.
  3. In the left part of the window, in the **General Settings** section, select the **Reports and Storages** subsection.
  4. In the right part of the window, under **Events to be included in the reports**, check the boxes for the types of events that should be included in the report.

CONFIGURING THE REMINDER OF REPORT AVAILABILITY

You can create a schedule, according to which Kaspersky Small Office Security reminds you about report readiness.

To create a schedule:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Small Office Security.
3. In the window that opens, on the **Report** tab, check the **Notify about the report** box and open the schedule settings window by clicking the link with the time setting.
4. In the **Report schedule** window that opens, specify the schedule settings.

NOTIFICATIONS

By default, if any events occur in operation, Kaspersky Small Office Security notifies you of them. If you are required to select further actions, notification windows will be displayed on the screen (see section "Notification windows and pop-up messages" on page 33). When encountering any events that do not require selecting actions, the application notifies you of them with sound signals, email messages, and pop-up messages in the taskbar notification area (see section "Notification windows and pop-up messages" on page 33).

You can select methods of notification (see section "Configuring the notification method" on page 223) of events or disable notifications (see section "Enabling and disabling notifications" on page 222).

IN THIS SECTION:

Enabling and disabling notifications 222

Configuring the notification method 223

ENABLING AND DISABLING NOTIFICATIONS

By default, Kaspersky Small Office Security uses various methods to notify you of all important events related to the application's operation (see section "Configuring the notification method" on page 223). You can disable the delivery of notifications.

Regardless of whether the notifications delivery is enabled or disabled, information about events that occur in the operation of Kaspersky Small Office Security, is logged in the application operation report.

When you disable the notifications delivery, it does not impact the display of notification windows. To minimize the number of notification windows displayed on the screen, use the automatic protection mode (see section "Using interactive protection mode" on page 39).

To enable or disable notifications delivery, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Notifications** subsection.
4. Uncheck the **Enable events notifications** box if notifications delivery should be disabled. Check this box if notifications delivery should be enabled.

CONFIGURING THE NOTIFICATION METHOD

The application notifies you of events using the following methods:

- pop-up messages in the taskbar notification area;
- sound notifications;
- email messages.

You can configure an individual set of notifications delivery methods for each type of events.

By default, critical notifications and notifications of application operation failures are accompanied with a sound signal. Microsoft Windows sound scheme is used as the source of sound effects. You can modify the current scheme or disable sounds.

To configure notifications delivery methods for various types of events:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Notifications** subsection.
4. In the right part of the window, check the **Enable events notifications** box and click the **Settings** button to the right.
5. In the **Notifications** window that opens, check boxes depending on how you want to be notified of various events: by email, with a pop-up message, or with a sound signal. To avoid receiving any notifications for a specified type of events, uncheck all boxes in the line corresponding to this event.

   To allow Kaspersky Small Office Security to notify you of events by email, you should adjust the email settings of notifications delivery.

To modify the email settings for notification delivering:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Notifications** subsection.
4. In the right part of the window, check the box **Enable email notifications** and click the **Settings** button to the right.
5. In the **Email notification settings** window that opens, specify the delivery settings.

To modify the sound scheme used with notifications, perform the following steps:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Notifications** subsection.
4. In the right part of the window, check the **Use Windows Default sound scheme** box and edit the scheme in your operating system.

   If the box is unchecked, the sound scheme from previous application versions is used.

To disable sound notifications:

1. Open themain application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Notifications** subsection.
4. In the right part of the window, uncheck the **Enable sound notifications** box.

PARTICIPATING IN THE KASPERSKY SECURITY NETWORK

A great number of new threats appear worldwide on a daily basis. You can join Kaspersky Security Network to speed up the collection of statistical data on types and sources of new threats and help develop methods to neutralize them.

Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about reputation of files, web resources, and software. Using data from Kaspersky Security Network ensures an increased response time of Kaspersky Small Office Security when encountering new types of threats, improves performance of some protection components, and reduces risk of false positives.

When you participate in Kaspersky Security Network, statistics collected while Kaspersky Small Office Security protects your computer are sent to Kaspersky Lab automatically.

No personal user data is collected, processed or stored.

Participating in the Kaspersky Security Network is voluntary. You should make your decision on participation while installing Kaspersky Small Office Security; however, you can change it any time later.

To enable Kaspersky Security Network:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **General Settings** section, select the **Feedback** subsection.
4. In the right part of the window, check the **I agree to participate in Kaspersky Security Network** box.

VALIDATING KASPERSKY SMALL OFFICE SECURITY SETTINGS

After Kaspersky Small Office Security has been installed and configured, you can verify if the application is configured correctly, using a test "virus" and its modifications. A separate test is required for each protection component / protocol.

IN THIS SECTION:

Test "virus" EICAR and its modifications 225

Testing the HTTP traffic protection 226

Testing the SMTP traffic protection 227

Validating File Anti-Virus settings 227

Validating virus scan task settings 227

Validating Anti-Spam settings 228

TEST "VIRUS" EICAR AND ITS MODIFICATIONS

This test "virus" has been specially developed by EICAR (The European Institute for Computer Antivirus Research) for testing anti-virus products.

The test "virus" IS NOT a real virus, because it does not contain code that can harm your computer. However, most anti-virus products identify EICAR as a virus.

Never use real viruses to test the operation of an anti-virus product!

You can download this test "virus" from the EICAR's official website at http://www.eicar.org/anti_virus_test_file.htm.

Before you download the file, you have to pause the computer's anti-virus protection, because otherwise the application would identify and process the test "virus" downloaded from the anti_virus_test_file.htm web page as an infected object transferred via HTTP.

The application identifies the file downloaded from the EICAR website as an infected object containing a virus that cannot be disinfected and performs the action selected for this type of object.

You can also modify the standard test "virus" to verify the operation of the application. To modify the "virus", change the content of the standard test "virus" by adding one of the prefixes to it (see table below). To modify the test "virus", you can use any text or hypertext editor, such as Microsoft Notepad or UltraEdit32.

First column of the table (see below) contains the prefixes, which should be added at the beginning of the standard test "virus" to create its modifications. The second column lists all possible statuses assigned to the object, based on the results of the scan by the application. The third column indicates how the application processes objects with the specified status. Please note that the actions performed in respect of the objects are determined by the application's settings.

Once you have added a prefix to the test "virus" save the resulting file under a name reflecting the "virus" modification, for example, having added the DELE- prefix, save the file as eicar_dele.com.

Make sure you have resumed anti-virus protection after downloading the test "virus" and creating its modifications.

Table 2. Modifications of the test virus

Prefix	Object status	Object processing information
No prefix, standard test "virus".	**Infected**. Object contains code of a known virus. Disinfection impossible.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed is that specified for non-disinfectable objects.
CORR-	**Corrupted**.	The application could access the object but could not scan it because it is corrupted (for example, the file structure is corrupted, or the file format is invalid). You can find the information that the object has been processed in the report on the application's operation.
WARN-	**Suspicious**. The object contains code of an unknown virus. Disinfection impossible.	The object has been considered suspicious. At the time of detection, the application databases contain no description of the procedure for disinfecting this object. You will be notified when an object of this type is detected.
SUSP-	**Suspicious**. The object contains modified code of a known virus. Disinfection impossible.	The application detected a partial correspondence of a section of object code with a section of code of a known virus. At the time of detection, the application databases contain no description of the procedure for disinfecting this object. You will be notified when an object of this type is detected.
ERRO-	**Scan error**.	An error occurred during the scan of an object. The application could not access the object, since the integrity of the object has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the object is scanned on a network resource). You can find the information that the object has been processed in the report on the application's operation.
CURE-	**Infected**. Object contains code of a known virus. Disinfectable.	Object contains a virus that can be disinfected. The application disinfects the object; the text of the virus body is replaced with the word CURE. You will be notified when an object of this type is detected.
DELE-	**Infected**. Object contains code of a known virus. Disinfection impossible.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed is that specified for non-disinfectable objects. You will be notified when an object of this type is detected.

TESTING THE HTTP TRAFFIC PROTECTION

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

- *In order to verify that viruses are successfully detected in a data stream transferred via the HTTP protocol:*

  try to download the test "virus" from the **EICAR**'s official website at http://www.eicar.org/anti_virus_test_file.htm.

When the computer attempts to download the test "virus", Kaspersky Small Office Security detects the object, identifies it as an infected object that cannot be disinfected, and performs the action specified in the HTTP traffic scan settings for objects with this status. By default, when you attempt to download the test "virus", the connection with the website is terminated and the browser displays a message indicating that the object is infected with the EICAR-Test-File virus.

TESTING THE SMTP TRAFFIC PROTECTION

In order to detect viruses in data streams transferred using SMTP protocol, you must use an email system that uses this protocol to transfer data.

You are advised to check virus detection in different parts of outgoing mail: in message body and in attachments. To check virus detection in message body, add the standard or modified EICAR test "virus" text to the message body.

To do so:

1. Create a **Plain text** format message using an email client installed on your computer.

A message that contains a test virus is not scanned if it is created in RTF or HTML format!

2. Insert the text of the standard or modified "virus" at the beginning of the message and attach the file containing the test "virus" to the message.
3. Send the message to the administrator.
4. Read the content of the message sent to this address.

Kaspersky Small Office Security detects the object, identifies it as an infected object, and performs the action specified in the SMTP traffic scan settings for this type of object. By default, messages with infected objects cannot be sent.

VALIDATING FILE ANTI-VIRUS SETTINGS

In order to verify that the File Anti-Virus configuration is correct:

1. Create a folder on the disk. Copy into this folder the test "virus" downloaded from the official **EICAR** website (http://www.eicar.org/anti_virus_test_file.htm) as well as all the test "virus" modifications you created.
2. Allow all events to be logged so the report file retains data on corrupted objects or objects skipped due to errors.
3. Run the test "virus" or one of its modified versions.

The File Anti-Virus intercepts the call to execute the file, scans it, and performs the action specified in the settings for objects of that status. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view information about the results of the File Anti-Virus operation in the report about the component's operation.

VALIDATING VIRUS SCAN TASK SETTINGS

In order to verify that the virus scan task is correctly configured:

1. Create a folder on the disk. Copy into this folder the test "virus" downloaded from the official **EICAR** website (http://www.eicar.org/anti_virus_test_file.htm) as well as all the test "virus" modifications you created.
2. Create a new virus scan task and select the folder containing the set of test "viruses" as the object to scan.
3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors.
4. Run the virus scan task.

When the scan task is running, the actions specified in the task settings are performed as suspicious or infected objects are detected. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view all information about the virus scan task actions in the report on the component's operation.

VALIDATING ANTI-SPAM SETTINGS

This section describes the functions of Kaspersky Small Office Security 2 for Personal Computer. These functions are missing in Kaspersky Small Office Security 2 for File Server.

You can use a test message identified as SPAM to test the anti-spam protection.

The body of the test message must contain the following line:

```
Spam is bad do not send it
```

When this message is received on the computer, Kaspersky Small Office Security scans it, assigns it the "spam" status, and performs the action specified for objects of this type.

CONTACTING THE TECHNICAL SUPPORT SERVICE

If problems occur during Kaspersky Small Office Security's operation, firstly check if the method for solving them is described in the documentation, help, Knowledge Base on the Kaspersky Lab Technical Support website, or on the User Forum.

If you cannot find a solution to your problem, please contact Kaspersky Lab Technical Support Service in one of the following ways:

- send a query with the help of the Personal Cabinet on the Technical Support Service website;
- by telephone.

Technical Support Service specialists will answer any of your questions about installing, activating and using the application. They will help you to eliminate the consequences of malware activities if your computer has been infected.

Before contacting the Technical Support Service, please read the Support rules for Kaspersky Lab's products (http://support.kaspersky.com/support/rules).

When you contact the Technical Support Service, service specialists may ask you to compile a report on the system status and a trace file and send them to the Technical Support Service. After Technical Support Service specialists analyze the data you have sent, they can create an AVZ script for you to help eliminate your problems.

IN THIS SECTION:

My Kaspersky Account 229

Technical support by phone 230

Creating a system state report 230

Creating a trace file 231

Sending data files 231

Executing AVZ script 232

MY KASPERSKY ACCOUNT

My Kaspersky Account – your personal section on the Technical Support Service website. Using My Kaspersky Account, you can perform the following actions:

- contact Technical Support Service and Virus Lab;
- contact the Technical Support Service without using the email;
- track the status of your request in real time;
- view a detailed history of your requests to the Technical Support Service.

To log in to My Kaspersky Account, use one of the following options:

- click the **My Kaspersky Account** link in the Kaspersky Small Office Security main window;

- in the address bar of your browser, type https://my.kaspersky.com.

If you do not have an account yet, you can register at the My Kaspersky Account registration page https://my.kaspersky.com/registration. Enter your email address and a password to log in to My Kaspersky Account. To send a request concerning Kaspersky Small Office Security usage, you will be asked to enter an activation code.

Note that some requests should not be addressed to the Technical Support Service, but instead to the Kaspersky Virus Lab. These are requests of the following types:

- unknown malicious program – you suspect that an object is malicious, while Kaspersky Small Office Security does not classify it that way;
- false alarm – Kaspersky Small Office Security classifies a file as a virus, yet you are sure that the file is not a virus;
- description of the malicious program – you want to get a description of a specified virus.

To send a request to the Virus Lab, you don't need to enter an activation code.

You do not need to be a registered user of My Kaspersky Account to be able to send requests to Kaspersky Virus Lab from the page with request form (http://support.kaspersky.com/virlab/helpdesk.html).

TECHNICAL SUPPORT BY PHONE

If you encounter a problem, which requires an urgent assistance, you can call your nearest Technical Support office. Before calling Russian-speaking (http://support.kaspersky.ru/support/support_local) or international (http://support.kaspersky.com/support/international) technical support specialists, please collect the information (http://support.kaspersky.com/support/details) about your computer and the anti-virus application on it. This will allow our specialists to help you more quickly.

CREATING A SYSTEM STATE REPORT

When solving your problems, Kaspersky Lab Technical Support Service specialists may require a report about the system status. This report contains detailed information about running processes, loaded modules and drivers, Microsoft Internet Explorer and Microsoft Windows Explorer plug-ins, open ports, detected suspicious objects, etc.

When a system state report is created, no personal user information is collected.

To create a system state report:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Support tools** link.
4. In the **Information for Technical Support Service** window that will open, click the **Create system state report** button.

The system state report is created in HTML and XML formats and is saved in the sysinfo.zip archive. Once the information has been gathered, you can view the report.

To view the report:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that will open, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that will open, click the **View** button.

5. Open the sysinfo.zip archive, which contains report files.

CREATING A TRACE FILE

After installing Kaspersky Small Office Security, some failures in the operating system or in the operation of individual applications may occur. The most likely cause is a conflict between Kaspersky Small Office Security and the software installed on your computer, or with the drivers of your computer components. You may be asked to create a trace file for Kaspersky Lab Technical Support Service specialists to successfully resolve your problem.

To create a trace file:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that will open, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that opens specify the trace level from the drop-down list in **Traces** section.

   It is recommended that the required trace level is clarified by a Technical Support Service specialist. In the absence of guidance from Technical Support Service, you are advised to set the trace level to **500**.

5. To start the trace process, click the **Enable** button.

6. Reproduce the situation which caused the problem to occur.

7. To stop the trace process, click the **Disable** button.

You can switch to uploading tracing results (see section "Sending data files" on page 231) to a Kaspersky Lab's server.

SENDING DATA FILES

After you have created the trace files and the system state report, you need to send them to Kaspersky Lab Technical Support Service experts.

You will need a request number to upload data files to the Technical Support Service server. This number is available in your Personal Cabinet on the Technical Support Service website if your request is active.

In order to upload the data files to the Support service server:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that will open, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that will open, in the **Actions** section, click the **Upload information for Technical Support Service to the server** button.

5. In the **Uploading information for Technical Support Service to the server** window that will open, check boxes next to the tracing files you wish to send to the Technical Support Service and click the **Send** button.

6. In the **Request number** window that will open specify the number assigned to your request when completing the electronic form at the Technical Support Service site.

The selected data files are packed and sent to the Technical Support Service server.

If for any reason it is not possible to contact the Technical Support Service, the data files can be stored on your computer and later sent from the Personal Cabinet.

To save data files on a disk:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Support tools** link.
4. In the **Information for Technical Support Service** window that will open, in the **Actions** section, click the **Upload information for Technical Support Service to the server** button.
5. In the **Uploading information for Technical Support Service to the server** window that will open, check boxes next to the tracing files you wish to send to the Technical Support Service and click the **Send** button.
6. Click the **Cancel** button in the **Request number** window that will open and confirm saving files to the disk by clicking **Yes**.
7. Specify the archive name in the window that will open and confirm saving.

The created archive can be sent to the Technical Support Service from the Personal Cabinet.

EXECUTING AVZ SCRIPT

Kaspersky Lab experts will analyze your problem using the trace files and the system state report. The outcome of the analysis is a sequence of actions aimed at removing the detected problems. The number of these actions can be very large.

To simplify the procedure, AVZ scripts are used. An AVZ script is a set of instructions that allow the editing of registry keys, quarantine of files, searching for classes of files and potentially quarantine files related to them, block UserMode and KernelMode interceptors, etc.

To run the scripts, the application includes an *AVZ script execution wizard*.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

You are advised not to change the text of an AVZ script received from Kaspersky Lab experts. If problems occur during script execution, please contact Technical Support Service.

To start the Wizard:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Support tools** link.
4. In the **Information for Technical Support Service** window that will open click the **Execute AVZ script** button.

If the script successfully executes, the Wizard closes. If an error occurs during script execution, the Wizard displays a corresponding error message.

APPENDIX

This section includes reference information which complements the document text.

IN THIS SECTION:

Subscription statuses 233

Working with the application from the command line 234

SUBSCRIPTION STATUSES

The following options are used to designate the subscription status:

- *Being defined*. Your request to activate the subscription has not yet been processed (some time is required for processing the request at the server). Kaspersky Small Office Security works in a full-functional mode. If after a certain period of time the subscription request has not been processed, you will receive notification that the subscription status update has not been performed. In this case the application databases will not be updated any longer (for license with update subscription), and neither will computer protection be performed (for license with protection and update subscription).

- *Active*. The subscription has been activated with no fixed term, or for a certain period of time (subscription expiry date is defined).

- *Renewed*. The subscription has been renewed with no fixed term, or for a certain period of time.

- *Error*. An error occurred when updating the subscription status.

- *Expired. Grace period.* Subscription expired, or status renewal term expired. If the status renewal term has expired, update the subscription status manually. If the subscription has expired, you can renew it, by contacting the online store from which you had purchased Kaspersky Small Office Security. To use a different activation code, you should first delete the license you are currently using.

- *Expired. Grace period expired.* Subscription expired, or grace period for license renewal expired. Please contact the subscription provider to purchase a new subscription, or to renew the existing one.

  If the subscription validity period has elapsed as well as the grace period during which license can be renewed (subscription status – *Expired*) Kaspersky Small Office Security will notify you about it and will stop its attempts to renew license automatically. For license with update subscription the functionality of the application will retain except for the databases update feature. For license with protection and update subscription the application databases will not be updated, computer protection will not be performed and scan tasks will not be executed.

- *Subscription cancellation.* You canceled subscription to automatic license renewal.

- *Update is required*. Subscription status has not been updated at the proper time for whatever reason.

  If the subscription has not been renewed in time (for example, the computer was turned off when license renewal was available), you can update its status manually in the license management window. Until the moment of subscription renewal, Kaspersky Small Office Security ceases to update the application databases (for license with update subscription) and stops performing computer protection or executing scan tasks (for license with protection subscription).

- *Suspended*. Subscription to automatic license renewal has been suspended.

- *Resumed*. Subscription has been resumed.

In some cases, additional information about the subscription status can be displayed for a license with subscription.

WORKING WITH THE APPLICATION FROM THE COMMAND LINE

You can work with Kaspersky Small Office Security from the command line. The capability is provided to perform the following operations:

- activate the application;
- start and stop the application;
- start and stop application components;
- start and stop the tasks;
- obtain information on the current status of components and tasks as well as their statistics;
- start and stop virus scan tasks;
- scan selected objects;
- update databases and software modules, roll back updates;
- export and import security settings;
- open help files using the command line syntax in general and for individual commands.

Command prompt syntax:

```
avp.com <command> [options]
```

You should access the application from the command line from the application installation folder, or by specifying the full path to avp.com.

The list of commands used to control the application and its components is provided in the table below.

START	Starts a component or a task.
STOP	Stops a component or a task. The command can only be executed if the password assigned via the Kaspersky Small Office Security interface is entered.
STATUS	Displays the current status of a component or task on the screen.
STATISTICS	Displays the statistics for a component or task on the screen.
HELP	Displays the list of commands and command syntax information.
SCAN	Scans objects for viruses.
UPDATE	Starts the application update.
ROLLBACK	Rolls back to the last Kaspersky Small Office Security update made. The command can only be executed if the password assigned via the Kaspersky Small Office Security interface is entered.

EXIT	Closes the application. The command can only be run if the password assigned via the application interface is entered.
IMPORT	Import application protection settings. The command can only be executed if the password assigned via the Kaspersky Small Office Security interface is entered.
EXPORT	Exports the application protection settings.

Each command requires its own specific set of settings.

IN THIS SECTION:

Activating the application 235

Starting the application 235

Stopping the application 236

Managing application components and tasks 236

Virus scan 238

Updating the application 240

Rolling back the last update 241

Exporting protection settings 241

Importing protection settings 242

Creating a trace file 242

Viewing Help 243

Return codes of the command line 243

ACTIVATING THE APPLICATION

You can activate Kaspersky Small Office Security using a key file.

Command syntax:

```
avp.com ADDKEY <filename>
```

The table below describes the settings of command performance.

<filename>	Application key file name with the *.key extension.

Example:

```
avp.com ADDKEY 1AA111A1.key
```

STARTING THE APPLICATION

Command syntax:

```
avp.com
```

STOPPING THE APPLICATION

Command syntax:

```
avp.com EXIT /password=<your_password>
```

Parameters description is provided in table below.

<your_password>	Application password specified in the interface.

Note that this command is not accepted without a password.

MANAGING APPLICATION COMPONENTS AND TASKS

Command syntax:

```
avp.com <command> <profile|task_name> [/R[A]:<report_file>]
avp.com STOP <profile|task_name> /password=<your_password> [/R[A]:<report_file>]
```

Descriptions of commands and settings are given in the table below.

<command>	You can manage Kaspersky Small Office Security components and tasks from the command prompt with the following commands: START – start a protection component or a task. STOP – stop a protection component or a task. STATUS – display the current status of a protection component or a task. STATISTICS – output statistics to the screen for a protection component or a task. Note that the STOP command will not be accepted without a password.
<profile|task_name>	You can specify any protection component of Kaspersky Small Office Security, component module, on-demand scan or update task as the value for the **<profile>** setting (the standard values used by the application are shown in the table below). You can specify the name of any on-demand scan or update task as the value for the **<task_name>** setting.
<your_password>	Application password specified in the interface.
/R[A]:<report_file>	**/R:<report_file>** – log only important events in the report. **/RA:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on screen, and all events are shown.

In the **<profile>** setting, you should specify one of the values given in the table below.

RTP	All protection components. The **avp.com START RTP** command runs all the protection components if the protection has been completely disabled. If the component has been disabled using the **STOP** command from the command prompt, it is not launched by the **avp.com START RTP** command. In order to start it, you should execute the **avp.com START <profile>** command, with the name of the specific protection component entered for **<profile>**. For example, **avp.com START FM**.
FW	Firewall.
HIPS	Security Zone (only in Kaspersky Small Office Security 2 for Personal Computer).
pdm	Proactive Defense (only in Kaspersky Small Office Security 2 for Personal Computer).
FM	File Anti-Virus.
EM	Mail Anti-Virus (only in Kaspersky Small Office Security 2 for Personal Computer).
WM	Web Anti-Virus (only in Kaspersky Small Office Security 2 for Personal Computer). Values for Web Anti-Virus subcomponents: **httpscan (HTTP)** – scan HTTP traffic; **sc** – scan scripts.
IM	IM Anti-Virus (only in Kaspersky Small Office Security 2 for Personal Computer).
AB	Anti-Banner (only in Kaspersky Small Office Security 2 for Personal Computer).
AS	Anti-Spam (only in Kaspersky Small Office Security 2 for Personal Computer).
PC	Web Policy Management (only in Kaspersky Small Office Security 2 for Personal Computer).
AP	Anti-Phishing (only in Kaspersky Small Office Security 2 for Personal Computer).
ids	Network Attack Blocker.
Updater	Update.
Rollback	Rolling back the last update.
Scan_My_Computer	Scan.
Scan_Objects	Custom Scan.
Scan_Quarantine	Quarantine scan.
Scan_Startup (STARTUP)	Startup Objects Scan.
Scan_Vulnerabilities (SECURITY)	Vulnerability Scan.

Components and tasks started from the command prompt are run with the settings configured in the application interface.

Examples:

- *To enable File Anti-Virus, enter the following command:*

  ```
  avp.com START FM
  ```

- *To stop computer scan, enter the following command:*

  ```
  avp.com STOP Scan_My_Computer /password=<your_password>
  ```

VIRUS SCAN

Starting a scan of a certain area for viruses and processing malicious objects from the command prompt generally looks as follows:

```
avp.com SCAN [<object scanned>] [<action>] [<file types>] [<exclusions>]
[<configuration file>] [<report settings>] [<advanced settings>]
```

To scan objects, you can also use the tasks created in the application by starting the one you need from the command line. The task will be run with the settings specified in the Kaspersky Small Office Security interface.

Parameters description is provided in table below.

<object to scan> – this parameter gives the list of objects that are scanned for malicious code. The parameter may include several space-separated values from the list provided.	
<files>	List of paths to the files and folders to be scanned. You can enter an absolute or relative path to the file. Items on the list are separated by a space. Comments: • If the object name contains a space, it must be placed in quotation marks. • If reference is made to a specific folder, all files in this folder are scanned.
/MEMORY	RAM objects.
/STARTUP	Startup objects.
/MAIL	Mailboxes.
/REMDRIVES	All removable media drives.
/FIXDRIVES	All internal drives.
/NETDRIVES	All network drives.
/QUARANTINE	Quarantined objects.

/ALL	Full computer scan.
/@:<filelist.lst>	Path to a file containing a list of objects and catalogs to be scanned. You can enter an absolute or relative path to the file with the list. The path must be placed without quotation marks even if it contains a space. File with the list of objects should be in a text format. Each scan object should be listed on a separate line. You are advised to specify absolute paths to scan objects in the file. When specifying a relative path, you specify the path relative to the executable file of an application, not relative to the file with the list of scan objects.
<action> – this parameter determines what action will be taken with malicious objects detected during the scan. If this parameter has not been defined, the default action is the one with the value for **/i8.** If you are working in automatic mode, then Kaspersky Small Office Security automatically applies the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. An action which corresponds to the **<action>** parameter value is ignored.	
/i0	Take no action in respect of the object; record information about it in the report.
/i1	Disinfect infected objects; skip if disinfection fails.
/i2	Disinfect infected objects; skip if disinfection fails; do not delete infected objects from compound objects; delete infected compound objects with executable headers (sfx archives).
/i3	Disinfect infected objects; skip if disinfection fails; delete all compound objects completely if infected embedded files cannot be deleted.
/i4	Delete infected objects. Delete all compound objects completely if the infected parts cannot be deleted.
/i8	Prompt the user for action if an infected object is detected.
/i9	Prompt the user for action at the end of the scan.
<file types> – this parameter defines the file types that are subject to an anti-virus scan. By default, if this parameter is not defined, only infected files by contents are scanned.	
/fe	Scan only infectable files by extension.
/fi	Scan only infectable files by contents.
/fa	Scan all files.
<exclusions> – this parameter defines objects that are excluded from the scan. The parameter may include several space-separated values from the list provided.	
-e:a	Do not scan archives.
-e:b	Do not scan email databases.
-e:m	Do not scan plain text emails.
-e:<filemask>	Do not scan objects, which match the mask.
-e:<seconds>	Skip objects that are scanned for longer than the time specified in the **<seconds>** parameter.
-es:<size>	Skip objects with size (in MB) exceeding the value specified in the **<size>** setting. This setting is only available for compound files (such as archives).

<configuration file> – defines the path to the configuration file that contains the application settings for the scan. The configuration file is in text format and contains the set of command line parameters for the anti-virus scan. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.	
/C:<file_name>	Use the settings' values specified in the **<file_name>** configuration file.
<report settings> – this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on screen, and all events are shown.	
/R:<report_file>	Log important events in this file only.
/RA:<report_file>	Log all events in this file.
<advanced settings> – settings that define the use of anti-virus scan technologies.	
/iChecker=<on|off>	Enable / disable the use of iChecker technology.
/iSwift=<on|off>	Enable / disable the use of iSwift technology.

Examples:

- *Start a scan of memory, Startup programs, mailboxes, the directories My Documents and Program Files and the file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Scan the objects listed in the file object2scan.txt, using the configuration file scan_setting.txt for the job. Use the scan_settings.txt configuration file. When the scan is complete, create a report to log all events:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

A sample configuration file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

UPDATING THE APPLICATION

The syntax for updating the modules of Kaspersky Small Office Security and application databases from the command line is as follows:

```
avp.com UPDATE [<update_source>] [/R[A]:<report_file>] [/C:<file_name>]
```

Parameters description is provided in table below.

<update_source>	HTTP or FTP server or network folder for downloading updates. The value for the parameter may be in the form of a full path to an update source or a URL. If a path is not selected, the update source will be taken from the application update settings.
/R[A]:<report_file>	**/R:<report_file>** – log only important events in the report. **/RA:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on the screen, and all events are shown.

/C:<file_name>	Path to the configuration file that contains the Kaspersky Small Office Security update settings. A configuration file is a file in plain text format containing a list of command-line parameters for an application update. You can enter an absolute or relative path to the file. If this parameter is not defined, the values for the settings in the application interface are used.

Examples:

- *Update application databases and record all events in a report:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Update the Kaspersky Small Office Security modules using the settings of updateapp.ini configuration file:*

```
avp.com UPDATE /C:updateapp.ini
```

A sample configuration file:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLING BACK THE LAST UPDATE

Command syntax:

```
avp.com ROLLBACK [/R[A]:<report_file>][/password=<your_password>]
```

Parameters description is provided in table below.

/R[A]:<report_file>	**/R:<report_file>** – log only important events in the report. **/RA:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on the screen, and all events are shown.
<your_password>	Application password specified in the interface.

Note that this command is not accepted without a password.

Example:

```
avp.com ROLLBACK /RA:rollback.txt /password=<your_password>
```

EXPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com EXPORT <profile> <filename>
```

The table below describes the settings of command performance.

<profile>	Component or task with the settings being exported. For the **<profile>** setting, you can use any value listed in the "Managing application components and tasks" Help section.
<filename>	Path to the file to which the Kaspersky Small Office Security settings are being exported. An absolute or a relative path may be specified. The configuration file is saved in binary format (DAT), if no other format is specified, or it is not specified at all; it can be used later to export application settings onto other computers. The configuration file can also be saved as a text file. To do so, type the *.txt* extension in the file name. Note that you cannot import protection settings from a text file. This file can only be used to specify the main settings for Kaspersky Small Office Security operation.

Example:

```
avp.com EXPORT RTP c:\settings.dat
```

IMPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com IMPORT <filename>[/password=<your_password>]
```

The table below describes the settings of command performance.

<filename>	Path to the file from which the Kaspersky Small Office Security settings are imported. An absolute or a relative path may be specified.
<your_password>	Kaspersky Small Office Security password specified in the application interface. Security parameters can only be imported from a binary file.

Note that this command is not accepted without a password.

Example:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

CREATING A TRACE FILE

Trace file creation may be required in case of problems in Kaspersky Small Office Security operation. This will help Technical Support Service specialists to diagnose problems more accurately.

We only recommend creating trace files for troubleshooting a specific problem. Regularly enabling traces may slow down your computer and fill up your hard drive.

Command syntax:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

Parameters description is provided in table below.

[on|off]	Enable / disable trace file creation.
[file]	Output trace to file.
<trace_level>	This value can be a value from 0 (minimum level, only critical messages) to 700 (maximum level, all messages). Technical Support will tell you what trace level you need when you contact Technical Support. If the level is not specified, we recommend setting the value to 500.

Examples:

- *To disable trace file creation:*

```
avp.com TRACE file off
```

- *To create a trace file to be sent to Technical Support with a maximum trace level of 500:*

```
avp.com TRACE file on 500
```

VIEWING HELP

The following command is used to view help about the command line syntax:

```
avp.com [ /? | HELP ]
```

You can use one of the following commands to view help information about the syntax of a specific command:

```
avp.com <command> /?
avp.com HELP <command>
```

RETURN CODES OF THE COMMAND LINE

This section describes the return codes of the command line (see table below). The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a certain type of task.

GENERAL RETURN CODES	
0	Operation completed successfully.
1	Invalid setting value.
2	Unknown error.
3	Task completion error.
4	Task cancelled.
VIRUS SCAN TASK RETURN CODES	
101	All dangerous objects processed.
102	Hazardous objects detected.

GLOSSARY

A

Activating the application

Switching the application into full-function mode. The user needs a license to activate the application.

Active license

The license currently used for the operation of a Kaspersky Lab application. The license defines the expiration date for full functionality and the license policy for the application. The application cannot have more than one license with the active status.

Additional license

A license that has been added for the operation of Kaspersky Lab application but has not been activated. The additional license enters into effect when the active license expires.

Administration server certificate

Certificate which allows Administration server authentication when connecting the Administration console to it and when exchanging data with users' computers. Administration server certificate is created at the installation of the Administration server, and is stored in the Cert subfolder of the application installation folder.

Alternate NTFS streams

NTFS data streams (alternate data streams) designed to contain additional attributes or file information.

Each file in an NTFS file system is a set of streams. One of them contains the file content that one is be able to view after opening the file, other streams (called alternate) are designed to contain meta information and ensure, for example, NTFS compatibility with other systems, such as an older file system by Macintosh called Hierarchical File System (HFS). Streams can be created, deleted, stored apart, renamed, and even run as a process.

Alternate streams can be used by intruders to transfer data secretly, or to steal them from a computer.

Application modules

Files included in the Kaspersky Lab installation package responsible for performing its main tasks. A particular executable module corresponds to each type of the task performed by the application (real-time protection, on-demand scan, updates). By running a full scan of your computer from the main window, you initiate the execution of this task's module.

Application settings

Application settings which are common for all task types, regulating the application's operation as a whole, such as application performance settings, report maintenance settings, backup storage settings.

Archive

File "containing" one or several other objects which may also be archives.

Available updates

A set of updates for Kaspersky Lab application modules including critical updates accumulated over a certain period of time and changes to the application's architecture.

B

Backup

Creating a backup copy of a file before any processing and putting the copy into the backup storage area with the possibility of restoring the file later, for example, to scan it with updated databases.

BACKUP STORAGE

Special storage designed to save backup copies of objects created before their first disinfection or deletion.

BASE OF SUSPICIOUS WEB ADDRESSES

List of web addresses, whose content can be considered to be potentially dangerous. The list is created by Kaspersky Lab specialists. It is regularly updated and is included in the Kaspersky Lab application package.

BLACK LIST OF KEY FILES

A database containing information on blacklisted Kaspersky Lab key files. Black list file content is updated together with the product databases.

BLOCKING THE OBJECT

Denying access to an object from external applications. A blocked object cannot be read, executed, changed, or deleted.

BOOT-VIRUS

A virus that infects the boot sectors of a computer's hard drive. The virus forces the system to load it into memory during reboot and to direct control to the virus code instead of the original boot loader code.

C

COMPRESSED FILE

An archive file that contains a decompression program and instructions for the operating system for executing.

CONTAINER

Encrypted object that is used to store confidential information. A container is a password-protected virtual removable drive, to which files and folders are moved.

Kaspersky Small Office Security should be installed on the computer to work with containers.

D

DANGEROUS OBJECT

Object containing a virus. You are advised not to access these objects, because it may result in an infection of your computer. Once an infected object is detected, we recommend that you disinfect it using one of Kaspersky Lab's applications, or delete it if disinfection is not possible.

DATABASE OF PHISHING WEB ADDRESSES

List of web addresses, which are defined as phishing by Kaspersky Lab specialists. The database is regularly updated and part of the Kaspersky Lab application.

DATABASE UPDATE

One of the functions performed by a Kaspersky Lab application that enables it to keep protection current. In doing so, the databases are downloaded from the Kaspersky Lab update servers onto the computer and are automatically connected to the application.

DATABASES

Databases created by Kaspersky Lab's experts and containing a detailed description of all current threats to computer security as well as methods used for their detection and disinfection. These databases are constantly updated by Kaspersky Lab as new threats appear.

DELETING AN OBJECT

The method of processing objects which ends in it being physically deleted from its original location (hard drive, folder, network resource). We recommend that this method be applied to dangerous objects which, for whatever reason, cannot be disinfected.

DISINFECTING OBJECTS ON RESTART

A method of processing infected objects that are being used by other applications at the moment of disinfection. Consists of creating a copy of the infected object, disinfecting the copy created, and replacing the original, infected object with the disinfected copy after the next system restart.

DISK BOOT SECTOR

A boot sector is a particular area on a computer's hard drive, floppy, or other data storage device. It contains information on the disc's file system and a boot loader program that is responsible for starting the operating system.

There exist a number of viruses that infect boot sectors, which are thus called boot viruses. The Kaspersky Lab application allows scanning boot sectors for viruses and disinfecting them if an infection is found.

DOMAIN NAME SERVICE (DNS)

Distributed system for converting the name of a host (a computer or other network device) to an IP address. DNS functions in TCP/IP networks. Particularly, DNS can also store and process reverse requests, by determining the name of a host by its IP address (PTR record). Resolution of DNS names is usually carried out by network applications, not by users.

DUAL-HOMED GATEWAY

Computer equipped with two network adapters (each of which is connected to different networks) transferring data from one network to the other.

E

EVENT SEVERITY LEVEL

Description of the event, logged during the operation of the Kaspersky Lab application. There exist four severity levels:

Critical event.

Functional failure.

Warning.

Information message.

Events of the same type may have different severity levels, depending on the situation when the event occurred.

EXCLUSION

Exclusion is an object excluded from the scan by Kaspersky Lab application. You can exclude files of certain formats, file masks, a certain area (for example, a folder or a program), application processes, or objects by threat type, according to the Virus Encyclopedia classification from the scan. Each task can be assigned a set of exclusions.

F

FALSE ALARM

Situation when Kaspersky Lab's application considers a non-infected object as infected due to its code similar to that of a virus.

FILE MASK

Representation of a file name and extension using wildcards. The two standard wildcards used in file masks are * and ?, where * represents any number of any characters and ? stands for any single character. Using these wildcards, you can represent any file. Note that the name and extension are always separated by a period.

H

HARDWARE PORT

Socket on a hardware component of a computer in which a cable or a plug can be connected (LPT port, serial port, USB port).

HEADER

The information in the beginning of a file or a message, which is comprised of low-level data on file (or message) status and processing. In particular, the email message header contains such data as information about the sender and recipient, and the date.

HEURISTIC ANALYZER

Technology designed for detecting threats that cannot be identified using the Kaspersky Lab application databases. It allows detecting objects suspected of being infected with an unknown virus or a new modification of known viruses.

The use of a heuristic analyzer detects up to 92% of threats. This mechanism is fairly effective and very rarely leads to false positives.

Files detected by the heuristic analyzer are considered suspicious.

HOOK

Subcomponent of the application responsible for scanning specific types of email. The set of interceptors specific to your installation depends on what role or what combination of roles the application is being deployed for.

I

ICHECKER TECHNOLOGY

iChecker is a technology that increases the speed of anti-virus scans by excluding objects that have remained unchanged since their last scan, provided that the scan parameters (the anti-virus database and settings) have not changed. The information for each file is stored in a special database. This technology is used in both real-time protection and on-demand scan modes.

For example, you have an archive scanned by Kaspersky Lab application and assigned the not infected status. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If you altered the archive content by adding a new object to it, modified the scan settings or updated the anti-virus database, the archive is re-scanned.

Limitations of iChecker technology:

this technology does not work with large-size files since it is faster to scan a file than check whether it was modified since it was last scanned;

the technology supports a limited number of formats (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

INCOMPATIBLE APPLICATION

An antivirus application from a third-party developer or a Kaspersky Lab application that does not support management through Kaspersky Small Office Security.

INFECTABLE OBJECT

An object which, due to its structure or format, can be used by intruders as a "container" to store and distribute a malicious object. As a rule, they are executable files, for example, files with the .com, .exe, .dll extensions, etc. The risk of activating malicious code in such files is fairly high.

INFECTED OBJECT

Object containing a malicious code. It is detected when a section of the object's code completely matches a section of the code of a known threat. Kaspersky Lab does not recommend using such objects since they may infect your computer.

INPUT/OUTPUT PORT

Serves in processors (such as Intel) for exchanging data with hardware components. The input/output port is associated with a certain hardware component, and allows applications to address it for data exchange.

INSTALLATION WITH A LOGON SCRIPT

Method of remote installation of Kaspersky Lab's applications which allows assigning the startup of remote installation task to an individual user account (or to several user accounts). Registering a user in a domain leads to an attempt to install the application on the client computer on which the user has been registered. This method is recommended for installing the applications on computers running under Microsoft Windows 98 / Me operating systems.

INTERNET PROTOCOL (IP)

The basic protocol for the Internet, used without change since the time of its development in 1974. It performs basic operations in transmitting data from one computer to another and serves as the foundation for higher-level protocols like TCP and UDP. It manages connection and error processing. Technologies such as NAT and masking make it possible to hide a large number of private networks using a small number of IP addresses (or even one address), which make it possible to respond to the demands of the constantly growing Internet using the relatively restricted IPv4 address space.

K

KASPERSKY LAB'S UPDATE SERVERS

A list of Kaspersky Lab's HTTP and FTP servers from which the application downloads databases and module updates to your computer.

KEY FILE

File with the .key extension, which is your personal "key", necessary for working with the Kaspersky Lab application. A key file is included with the product if you purchased it from Kaspersky Lab distributors or is emailed to you if you purchased the product online.

L

LICENSE VALIDITY PERIOD

Period of time during which you are able to use all features of your Kaspersky Lab application. The license validity period generally runs for one calendar year from the date of installation. After the license expires, the application has reduced functionality. You will not be able to update the application databases.

LIST OF ALLOWED URLS

List of masks and addresses of web resources, the accessing of which is not blocked by the Kaspersky Lab application. The list of addresses is created by the user during application settings configuration.

LIST OF ALLOWED SENDERS

(as well as "White" list of addresses)

The list of email addresses which send the messages that should not be scanned by Kaspersky Lab application.

LIST OF BLOCKED URLS

List of masks and addresses of web resources, access to which is blocked by the Kaspersky Lab application. The list of addresses is created by the user during application settings configuration.

LIST OF BLOCKED SENDERS

(also "Black" list of addresses)

The list of email addresses which send messages that should be blocked by the Kaspersky Lab application, regardless of their content.

LIST OF CHECKED WEB ADDRESSES

List of masks and addresses of web resources, which are mandatorily scanned for malicious objects by the Kaspersky Lab application.

LIST OF TRUSTED URLS

List of masks and addresses of web resources whose content the user trusts. Kaspersky Lab application does not scan web pages, corresponding to a list item, for the presence of malicious objects.

M

MAIL DATABASES

Databases containing emails in a special format and saved on your computer. Each incoming/outgoing email is placed in the mail database after it is received/sent. These databases are scanned during a full computer scan.

Incoming and outgoing emails at the time that they are sent and received are analyzed for viruses in real time if real-time protection is enabled.

MESSAGE DELETION

Method of processing an email message, at which the message is physically removed. This method is recommended to apply to messages that definitely contain spam or malware. Before deleting a message, a copy of it is saved in the backup (unless this option is disabled).

MONITORED OBJECT

A file transferred via HTTP, FTP, or SMTP protocols across the firewall and sent to a Kaspersky Lab application to be scanned.

MOVING OBJECTS TO QUARANTINE

A method of processing a potentially infected object by blocking access to the file and moving it from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection.

N

NETWORK PORT

TCP and UDP parameter that determines the destination of data packets in IP format that are transmitted to a host over a network and makes it possible for various programs running on a single host to receive data independently of each other. Each program processes data received via a certain port (this is sometimes referred to as the program "listening" to that port).

For some common network protocols there are usually standard port numbers (for example, web servers usually receive HTTP requests on TCP port 80); however, generally, a program can use any protocol on any port. Possible values: 1 to 65535.

NOTIFICATION TEMPLATE

Template based on which a notification of infected objects detected by the scan, is generated. Notification template includes a combination of settings regulating the mode of notification, the way of spreading, and the text of messages to be sent.

O

OLE OBJECT

An attached object or an object embedded into another file. Kaspersky Lab application allows scanning OLE objects for viruses. For example, if you insert a Microsoft Office Excel table into a Microsoft Office Word document, the table is scanned as an OLE object.

OBJECT DISINFECTION

The method used for processing infected objects that results in complete or partial recovery of data, or the decision that the objects cannot be disinfected. Objects are disinfected using the database records. Part of the data may be lost during disinfection.

OBSCENE MESSAGE

Email message containing offensive language.

P

POTENTIALLY INFECTED OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Potentially infected files are detected using heuristic analyzer.

PROTECTION STATE

The current status of protection, summarizing the degree of security of the computer.

PROTOCOL

Clearly defined and standardized set of rules governing the interaction between a client and a server. Well-known protocols and the services associated with them include HTTP (WWW), FTP, and NNTP (news).

PROXY SERVER

Computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then, the proxy server either connects to the specified server and obtains the resource from it, or returns the resource from its own cache (in case if the proxy has its own cache). In some cases, a user's request or a server's response can be modified by the proxy server in certain reasons.

Q

QUARANTINE

A certain folder, where all possibly infected objects are placed, which were detected during scans or by real-time protection.

R

REAL-TIME PROTECTION

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or suspected of containing them are processed pursuant to the task settings (they are disinfected, deleted or quarantined).

RECOMMENDED LEVEL

Level of security based on application settings recommended by Kaspersky Lab experts to provide the optimal level of protection for your computer. This level is set to be used by default.

RESTORATION

Moving an original object from Quarantine or Backup to the folder where it was originally found before being moved to Quarantine, disinfected, or deleted, or to a different folder specified by the user.

S

SELECT THE

SOCKS

Proxy server protocol that allows establishing a point-to-point connection between computers in the internal and external networks.

SCRIPT

A small computer program or an independent part of a program (function) which, as a rule, has been developed to execute a small specific task. It is most often used with programs embedded into hypertext. Scripts are run, for example, when you open a certain website.

If real-time protection is enabled, the application tracks the scripts launching, intercepts and scans them for viruses. Depending on the results of the scan, you may block or allow the execution of a script.

SECURITY LEVEL

The security level is defined as a pre-set component configuration.

SPAM

Unsolicited mass email mailings, most often including advertising messages.

STARTUP OBJECTS

The set of programs needed to start and correctly operate the operating system and software installed on your computer. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which may lead to, for example, blocking your access to the operating system.

SUBNET MASK

Subnet mask (also known as netmask) and network address determine the addresses of computers on a network.

SUSPICIOUS MESSAGE

Message that cannot be unambiguously considered spam, but it seems suspicious when scanned (e.g., certain types of mailings and advertising messages).

SUSPICIOUS OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Suspicious objects are detected using the heuristic analyzer.

T

TASK

Functions performed by Kaspersky Lab's application are implemented as tasks, such as: Real-time file protection, Full computer scan, Database update.

TASK SETTINGS

Application settings which are specific for each task type.

TRAFFIC SCAN

A real-time scan using information from the latest version of the databases for objects transmitted via all protocols (for example, HTTP, FTP, etc.).

TRUSTED PROCESS

Application process whose file operations are not monitored by Kaspersky Lab's application in real-time protection mode. In other words, no objects run, open, or saved by the trusted process are scanned.

U

UNKNOWN VIRUS

A new virus about which there is no information in the databases. Generally unknown viruses are detected by the application in objects using the heuristic analyzer, and those objects are classified as potentially infected.

UPDATE

The procedure of replacing/adding new files (databases or application modules) retrieved from the Kaspersky Lab update servers.

UPDATE PACKAGE

File package for updating the software. It is downloaded from the Internet and installed on your computer.

URGENT UPDATES

Critical updates to Kaspersky Lab application modules.

V

VIRUS ACTIVITY THRESHOLD

The maximum permissible level of a specific type of event over a limited time period that, when exceeded, is considered to be excessive virus activity and a threat of a virus outbreak. This feature is significant during virus outbreaks and enables an administrator to react in a timely fashion to threats of virus outbreaks that arise.

VIRUS OUTBREAK

A series of deliberate attempts to infect a computer with a virus.

VIRUS OUTBREAK COUNTER

Template based on which a notification of virus outbreak threat is generated. Virus outbreak counter includes a combination of settings which determine the virus activity threshold, the way of spreading, and the text in messages to be sent.

KASPERSKY LAB

Kaspersky Lab is an internationally renowned company that creates software products to protect computers against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). According to a COMCON survey entitled TGI-Russia 2009, Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia.

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop and pocket computers, and for smartphones and other mobile devices.

The company delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly*; and the *Anti-Spam database every five minutes*.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers user the Kaspersky Anti-Virus kernel in their products, including: Safenet (USA), Alt-N (USA), Blue Coat (USA), Check Point (Israel), Clearswift (UK), Communigate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), Finjan (USA), GFI (Malta), IBM (USA), Juniper (USA), LANDesk (USA), Microsoft (USA), Netasq (France), Netgear (USA), Parallels (Russia), Sonicwall (USA), WatchGuard (USA), ZyXEL (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received the top Advanced+ award in a test carried out by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab's website:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.securelist.com
Anti-Virus Lab:	newvirus@kaspersky.com
	(only for sending suspicious files in archive format)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en
	(for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

INFORMATION ABOUT THIRD-PARTY CODE

Third-party code was used during the application development.

IN THIS SECTION:

Program code 254

Other information 272

PROGRAM CODE

Information about third-party code used during application development.

IN THIS SECTION:

AGG (ANTI-GRAIN GEOMETRY) 2.4 255
BISON PARSER SKELETON 2.3 256
BOOST 1.30.0, 1.39.0, 1.43.0 256
BZIP2/LIBBZIP2 1.0.5 257
EXPAT 1.2, 2.0.1 257
FASTSCRIPT 1.9 257
GECKO SDK 1.8 257
INFO-ZIP 5.51 257
LIBJPEG 6B 258
LIBNKFM 2.0.5 259
LIBPNG 1.2.8, 1.2.29 259
LIBSPF2 1.2.9 259
LIBUNGIF 3.0 260
LIBXDR 260
NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE 260
NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER 261
NETWORK CONFIGURATION SAMPLE 261
OPENSSL 0.9.8D 261
PCRE 3.0, 7.4, 7.7 262
PROTOCOL BUFFER 263
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 263
TINICONV 1.0.0 263
WINDOWS TEMPLATE LIBRARY 7.5 269
WINDOWS TEMPLATE LIBRARY 8.0 272
ZLIB 1.2, 1.2.2 272

AGG (ANTI-GRAIN GEOMETRY) 2.4

Copyright (C) 2002-2005, Maxim Shemanarev

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BISON PARSER SKELETON 2.3

Copyright (C) GNU Project

----

http://ftp.gnu.org/gnu/bison/

As a special exception, you may create a larger work that containspart or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BOOST 1.30.0, 1.39.0, 1.43.0

Copyright (C) Beman Dawes

BZIP2/LIBBZIP2 1.0.5

Copyright (C) 1996-2007 Julian R Seward.

EXPAT 1.2, 2.0.1

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FASTSCRIPT 1.9

Copyright (C) Fast Reports Inc

GECKO SDK 1.8

Copyright (C) Mozilla Foundation

---

http://www.mozilla.org/MPL/MPL-1.1.html

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip, "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBJPEG 6B

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBNKFM 2.0.5

Copyright (C) KUBO Takehiro

LIBPNG 1.2.8, 1.2.29

Copyright (C) 2004, 2006-2008, Glenn Randers-Pehrson

LIBSPF2 1.2.9

Copyright (C) 2005, Shevek and Wayne Schlitt

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,

STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBUNGIF 3.0

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR

Copyright (C) Sun Microsystems, Inc

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE

Copyright (C) 1992-2000, Microsoft Corporation

NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER

Copyright (C) 2004-2005, Microsoft Corporation

NETWORK CONFIGURATION SAMPLE

Copyright (C) 1997, Microsoft Corporation

OPENSSL 0.9.8D

Copyright (C) 1998-2007, The OpenSSL Project

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence

[including the GNU Public Licence.]

PCRE 3.0, 7.4, 7.7

Copyright (C) University of Cambridge

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PROTOCOL BUFFER

Copyright (C) 2008, Google Inc

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

TINICONV 1.0.0

Copyright (C) Free Software Foundation, Inc

---

http://sourceforge.net/projects/tiniconv/

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

WINDOWS TEMPLATE LIBRARY 7.5

Copyright (C) 2005, Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions

brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

WINDOWS TEMPLATE LIBRARY 8.0

Copyright (C) Microsoft Corporation

ZLIB 1.2, 1.2.2

Copyright (C) Jean-loup Gailly and Mark Adler

OTHER INFORMATION

Additional information about third-party code.

Agava-C program library, developed by OOO "R-Alpha", is used to check digital signature.

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software.

INDEX

A

Additional Tools
- Browser Configuration 216
- Delete Unused Data 215
- Permanently Delete Data....212
- Privacy Cleaner Wizard 214

Anti-Banner
- list of allowed banner addresses 114
- white list....114

Anti-Spam
- filtering email messages at the server 110
- list of allowed phrases 104
- list of allowed senders 105
- plug-in for Microsoft Office Outlook 111
- plug-in for Microsoft Outlook Express....112
- plug-in for The Bat! 112
- plug-in for Thunderbird 113

B

Backup
- clearing a storage....147
- connecting a storage 146
- creating a backup task....148
- creating a storage....146
- removing a storage....147
- restoring data....149
- running a backup task 148
- searching for backup copies....150
- viewing backup copy data....151
- viewing event report 151

D

Data Encryption
- adding files into container....164
- configuring container 164
- connecting and disconnecting container....162
- creating a container 161

Detectable threat categories 207

F

Firewall
- extending the range of network addresses....128
- Rule Creation Wizard 129

I

Inheriting rights
- Security Zone 122

L

License
- End User License Agreement....26

M

Mail Dispatcher
- Anti-Spam....110

Management Console
backup....169
configuring remote management....166
managing licenses....170
managing protection components....168
scanning for viruses and vulnerabilities....167
updating....167
Mode selection
Safe Run....141

N

Network Attack Blocker
types of detected network attacks....131

P

Password Manager
Accessing Password Database....176
Caption Button....201
changing Master Password....199
encryption method....196
finding passwords....185
group of accounts....182
Identity....183
importing / exporting passwords....186
Password Generator....203
Portable Version....204
private data....184
quick launch of functions....194
user name....183

R

Reports....218

S

Safe Run
mode selection....141
shortcut creation....141
Security Zone
inheriting rights....122
Security Zone rules....119
Security Zone rules
Security Zone....119
Shortcut creation
Safe Run....141

U

Update
proxy server....76
regional settings....74
rolling back the last update....76
update source....73
Updating
scheduled updates....75
Updating from a local folder....74
Updating the application....72

W

Web Policy Management
access to web sites....156
downloading files from the Internet....157

enabling and configuring....153
exporting / importing the settings....154
instant messaging....158
key words search....160
limiting computer usage time....155
limiting time of Internet access....156
running applications and games....156
safe search mode....157
sending private data....160